Department of Energy
CIAC
Computer Incident Advisory Capability

UCRL-MA-115896 Rev. 2

Virus Information Update
CIAC-2301

Steve Cooper
William J. Orvis

March 1996

Lawrence Livermore National Laboratory

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, shortly after the Internet Worm, CIAC provides various computer security services to employees and contractors of the DOE, such as:

- Incident Handling consulting
- Computer Security Information
- On-site Workshops
- White-hat Audits

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

The CIAC Computer Virus Information Update

Introduction

Purpose of this document

While CIAC periodically issues bulletins about specific computer viruses, these bulletins do not cover all the computer viruses that affect desktop computers. The purpose of this document is to identify most of the known viruses for the MS-DOS and Macintosh platforms and give an overview of the effects of each virus. We also include information on some Windows, Atari, and Amiga viruses. This document is revised periodically as new virus information becomes available. This document replaces all earlier versions of the CIAC Computer Virus Information Update. The date on the front cover indicates date on which the information in this document was extracted from CIAC's Virus database.

What's in this document

The CIAC computer virus database contains information about small computer viruses and Trojans. There are eleven tables in this document. The first five tables contain computer virus information for the Macintosh, PC-DOS/MS-DOS, Windows, Amiga, and Atari computers. The sixth table is a list of known viruses for which we do not yet have any information in the main tables.

Because there are so many PC-DOS/MS-DOS virus names and aliases, the seventh table is a cross-reference of PC-DOS/MS-DOS virus names and aliases. To locate a PC virus by name, find the name in the first column of the cross-reference table. The name given in the second column is the virus name we have used in the PC-DOS/MS-DOS computer virus table. All the virus tables are sorted in alphabetical order by the virus name.

The last four tables contain expanded definitions for descriptions used in the virus description tables.

While we include a separate table for Windows viruses, a PC running Windows is generally susceptible to all the viruses in the MS-DOS/PC-DOS Viruses Table. We have not yet seen OS/2 or Windows NT viruses, though we have heard rumors of one or two. OS/2 and Windows NT will generally not be susceptible to MS-DOS/PC-DOS viruses, except when they have a PC compatibility window open, or have a DOS type file system. As a rule of thumb, anywhere a MS-DOS program can run a MS-DOS virus can also run.

Information sources

Please keep in mind that these tables are made with the most recent information that we have, but they are not all based on first-hand experience. We depend on many sources of information, some of which include:

- Dr. Klaus Brunnstein and Simone Fischer-Huebner, Virus Test Center, Faculty for Informatics, University of Hamburg
- Dave Chess, IBM
- Bill Couture, Digital Dispatch Inc.
- Joe Hirst, British Computer Virus Research Center
- McAfee Associates
- John Norstad, Academic Computing and Network Services, Northwestern University
- Fridrik Skulason, FRISK Software International.
- Gene Spafford, Purdue University
- Joe Wells, IBM
- CERT, the Computer Emergency Response Team at the Software Engineering Institute, Carnegie-Mellon University
- VIRUS-L, the virus news service moderated by Ken Van Wyk
- FIRST, the Forum of Incident Response & Security Teams
- And the people in the Department of Energy and its contractors.

Some of the information is hearsay in nature, but is included because we felt it was reliable. We believe that reliable hearsay information is better than nothing when dealing with a computer virus.

Anti-Virus Software Availability

Availability	There are numerous commercial and shareware anti-virus packages available for both Macintosh and MS-DOS computers. If you have Internet access, the public domain and shareware packages are available on many of the anonymous FTP file servers. Several of these products are available in the CIAC Archive (see “Additional Information and Assistance” below).
MS-DOS computers	For MS-DOS based computers, the Department of Energy has purchased a site-license for DDI’s Data Physician Plus! package. This is available at no charge to all DOE personnel and their contractors for official use at DOE and contractor sites. Contact your computer security operations office for details on how to obtain a copy for your use.
Macintosh computers	For Macintosh computers, the freeware package Disinfectant is available from John Norstad at Northwestern University. CIAC tries to maintain the latest copy in the CIAC Archive (see “Additional Information and Assistance” below.) You can also obtain a copy directly from Northwestern University using anonymous FTP to ftp.acns.nwu.edu. Be sure to tell John, "thank you, " whenever you get the chance.
Macintosh PC Emulator	For Macintosh computers, running the SoftPC emulator, or Mac PowerPCs running SoftWindows, you need to scan the Macintosh portion of the file system with a Macintosh virus scanner and the PC portion of the file system with a PC virus scanner. When SoftPC or SoftWindows is installed, it creates a file in the Macintosh file system to use as the PC hard disk. While a Macintosh virus scanner can scan this file, it does not know how to detect PC viruses there. To scan the PC part of the disk, run the PC emulator and then run a PC virus scanner within the PC emulation.
Updates	Please keep in mind that anti-virus software must be periodically updated to be effective against new computer viruses. Also, if you use a shareware package, do not forget to compensate the author. The cost is minimal for the functionality you receive.

Macro Viruses

A new class of viruses was discovered this year that infect Microsoft Word documents. These are the so called Winword Macro viruses and are listed in the Windows Viruses Table. While these viruses were primarily written to infect Word for Windows documents, they actually infect any machine that can run Word version 6 or later. This includes Windows 3.1, Windows 95, Windows NT, and Macintosh.

Macro Viruses

A macro virus is a piece of self-replicating code written in an application's macro language. Many applications have macro capabilities such as the automatic playback of keystrokes available in early versions of Lotus 1-2-3. The distinguishing factor which makes it possible to create a virus with a macro is the existence of auto-execute macros in the language. An auto-execute macro is one which is executed in response to some event and not in response to an explicit user command. Common auto-execute events are opening a file, closing a file, and starting an application. Once a macro is running, it can copy itself to other documents, delete files, and create general havoc in a person's system. These things occur without the user explicitly running the macro.

Another type of hazardous macro is one named for an existing Word command. If a macro in the global macro file or in an attached, active template has the name of an existing Word command, the macro command replaces the Word command. For example, if you create a macro named FileSave in the "normal.dot" template, that macro is executed whenever you choose the Save command on the File menu. There is no way to disable this feature.

Macro viruses spread by having one or more auto-execute macros in a document. By opening or closing the document or using a replaced command, you activate the virus macro. As soon as the macro is activated, it copies itself and any other macros it needs to the global macro file "normal.dot". After they are stored in normal.dot they are available in all opened documents.

An important point to make here is that Word documents (.DOC files) can not contain macros, only Word templates (.DOT files) can contain macros. However, it is a relatively simple task to mask a template as a document by changing the file name extension from .DOT to .DOC.

Protecting A System From Macro Viruses

Currently, the best protection is to install Microsoft's macro virus protection template. The template is available directly from Microsoft's web site or from the CIAC archive. The template works on Macintosh versions of Word 6 as well as on Windows versions. A description and the template are available at:

http://www.microsoft.com/msoffice/freestuf/ msword/download/mvtool/mvtool2.htm
http://www.microsoft.com/msoffice/freestuf/msword/download/mvtool/mvtool10.exe

WARNING: The template from Microsoft only scans files if they are opened with the File-Open command in Word and not if they are opened by double-clicking the document or by selecting the document from the recent documents list at the bottom of the File menu. You must use the File-Open command to activate the protection.

The Virus Tables

The computer viruses in the first five tables in this document are described in the format shown below. In most cases, short phrases are used to describe the type, features, and other characteristics of the virus. The last four tables in this document expand on the phrases used in the virus tables.

<table>
<tr><td>Name: The name of the virus used in this report. Note that virus names are not unique, and that the same virus may be known by more than one name. The virus descriptions are sorted alphabetically by the first name in this field.</td><td colspan="3"></td></tr>
<tr><td>Aliases: This field gives the different names by which the virus is known, including different names for the same virus, and the names of any nearly identical variants (clones).</td><td colspan="3">Type: The virus is classified here according to where it hides or how it attacks a system.</td></tr>
<tr><td colspan="2">Disk Location: This field describes where the virus hides on a disk, which is generally the vehicle by which it is transferred to another machine. For Trojans, the name of the Trojan program is also listed here.</td><td colspan="2">Features: This field describes where the virus hides in memory and how it infects new disks. Included here are any special features, such as encryption and stealth capabilities.</td></tr>
<tr><td colspan="2">Damage: This field describes the intentional and unintentional damage done by the virus.</td><td>Size: This field describes any changes that a virus makes to other programs and data on disk, especially increases in file length. Not all viruses increase the length of an infected file.</td><td>See Also: This field points to related virus descriptions that may contain more information.</td></tr>
<tr><td colspan="4">Notes: This field contains descriptive information, information on how to detect and eradicate a virus, and any information that does not fit in the categories above.</td></tr>
</table>

Additional Information and Assistance

From CIAC

DOE sites and contractors and the NIH may obtain additional information or assistance from CIAC:

- Phone: (510) 422-8193
- FAX: (510) 423-8002
- Internet: ciac@llnl.gov

Other agencies should contact their respective response teams (See FIRST below.)

From the CIAC Archive

Anti-virus documents and software are available from the CIAC archive.

- WWW access to **http://ciac.llnl.gov**
- FTP access to **ciac.llnl.gov** using the Internet (IP address 128.115.19.60) and anonymous FTP. Log in with FTP, use "anonymous" as the user name and your E-mail address as the password.
- Telephone access via the **CIAC BBS** at 28.8K baud at (510) 423-4753 or at (510) 423-3331 (8 bit, no parity, 1 stop bit).

FIRST

If you don't know who your response team is, contact the Forum of Incident Response and Security Teams (FIRST). FIRST is a world-wide organization of computer security response teams from the public, government and academia. A list of FIRST member organizations and their constituencies can be obtained by sending e-mail to docserver@first.org with an empty subject line and a message body containing the line: send first-contacts.

For Emergencies

DOE sites and contractors and the NIH may use the CIAC Sky Page in case of an emergency. To use the Sky Page, call 1-800-SKYPAGE and enter PIN number 855-0070 or 855-0074.

Macintosh Computer Virus Table

Name: Aliens 4		
Aliases: Aliens 4	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: NOT A VIRUS! August 17, 1992 the DISA office published a Defense Data Network Security Bulletin about this non-virus. Quote: "It's fast, It mutates, It likes to travel, Every time you think you've eradicated it, it pops up somewhere else." They gave no way to identify it, and suggested you reformat your macintosh. No Mac anti-virus people were contacted before sending this alert out. On August 23, the alert was cancelled with a epilogue note. All this was sent out on the Internet, so it is fairly far-reaching.		

Name: ANTI		
Aliases: ANTI, ANTI-ANGE, ANTI A, ANTI B	**Type:** Patched CODE resource.	
Disk Location: Application programs and Finder.	**Features:**	
Damage: Interferes with a running application.	**Size:**	**See Also:**
Notes: Attacks only application files, and causes some problems with infected applications. VirusDetective search string: Resource Start & Pos -1100 & WData 000FA146#90F#80703 ; For finding ANTI A & B SAM def: Name=ANTI, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=000A317CFFFF000CA033303C0997A146, String Offset=any		

Name: April Fools		
Aliases: April Fools	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: April Fools causes a system bomb alert box to appear when an alert box is supposed to. The bomb message says "Error: Initializing hard disk..." and is accompanied by a few seconds of the startup disk being accessed. Then an April Fools message appears followed by the normal alert box. After two executions, the program disables itself. To remove, remove from the System (Extensions) Folder and restart.		

Name: Backwords		
Aliases: Backwords	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: The Mac displays all text in reverse, including names, menus, and word processing text. Also, text typed in is in reverse. To remove, look for and remove the extension with the backwords B icon in the Systems extensions folder (remembering that all these names will be displayed backwords). Then restart using "tratseR" from "laicepS" menu (Restart from Special menu).		

Name: Blue Meanie		
Aliases: Blue Meanie, Brian McGhie	**Type:** Other: Not a virus	
Disk Location: System program.	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: A programmer apparently left the following text in the system file as a joke. It is in the second sector of thedata fork of the system. Maybe these are the apple programmers that worked on the system.

==========

Help! Help! He's STILL being held prisoner in a system software factory!

The Blue Meanie:

Brian McGhie

Also serving time:

Giovanni Agnoli
Eric3 Anderson
Jeff Crawford
Cameron Esfahani
Dave Falkenburg
Hoon Im
Dave Lyons
Mike Larson
Darren Litzinger
Rob lunatic Moore
Jim Murphy
Mike Puckett
Anumele Raja
Jim Reekes
Alex Rosenberg
Eric Slosser
Randy theLen
Steve Stevenson
Roshi Yousefi

and Tristan Farnon (because he paid us ten bucks)

Fugitives:
Lars Borresen
Scott Boyd
Jaime Cummins
Brad Post

Will the last person to leave please turn off the lights?
Joy

Name: BrokaMac		
Aliases: BrokaMac	**Type:** Joke program, not a virus.	
Disk Location: Startup Item	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Simulates hardware failure by presenting blurry desktop and generating squeeling noise. CAPS LOCK key or, on microphone equipped Macs, a loud noise causes BrokaMac to exit. Remove by starting with extensions off and removing from system Startup Items folder (System 7) or locate it and drag it to the trash (System 6).		

Name: Burning Fuse		
Aliases: Burning Fuse	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This extension causes an animation of a bomb with a burning fuse to appear when the user selects Shutdown or Restart. The cursor appears as a lit match. When the fuse burns down, it generates an explosion noise and then proceeds normally. To remove, remove it from the System (Extensions) Menu and restart.		

Name: CDEF		
Aliases: CDEF	**Type:** Bogus resource. CDEF	
Disk Location: The Desktop file	**Features:**	
Damage: No damage, only replicates.	**Size:** CDEF ID#1 in Desktop File	**See Also:** WDEF
Notes: It only infects the invisible "Desktop" files used by the Finder. Infection can occur as soon as a disk is inserted into a computer. An application does not have to be run to cause an infection. It does not infect applications, document files, or other system files. The virus does not intentionally try to do any damage, but still causes problems with running applications. Like WDEF, does not infect System 7 (virus-l, v4-223) VirusDetective search string: Creator=ERIK & Executables ; For finding executables in the Desktop Find CDEF ID=1 in the Desktop file. SAM def: Name=CDEF, Resource type=CDEF, Resource ID=1, Resource Size=510, Search String=45463F3C0001487A0046A9AB, String Offset=420 Rebuild the Desktop - Hold down Command and Option while inserting the disk.		

Name: CODE 252		
Aliases: CODE 252	**Type:** Bogus CODE resource.	
Disk Location: System program.Application programs and Finder.	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**

Notes: This virus triggers if an infected application is run or system booted between JUNE6 and DECEMBER 31. Between Jan 1 and June 6 the virus simply replicates.
Under System 7, the System file can be seriously damaged by this virus as it spreads. This damage may cause a system to not boot, crash, or other unusual behavior.
The virus does not spread to other applications under MultiFinder on System 6.x systems, and does not spread at all under System 7, HOWEVER, it will run if a pre-infected application is executed. When triggered, a message appears in a dialog box that says all disks are being erased, but NO ERASURE TAKES PLACE. Disinfectant 2.8, Gatekeeper 1.2.6 (but earlier versions can find virus, just not by name), Rival 1.1.9v,
SAM 3.0.8, Virex INIT 3.8, Virus Detective 5.0.4, also after June 6, if you see the message Disinfectant 2.8, Gatekeeper 1.2.6, Rival 1.1.9v, SAM 3.0.8, Virex INIT 3.8, Virus Detective 5.0.4
The message displayed is:

You have a virus.
Ha Ha Ha Ha Ha Ha Ha
Now erasing all disks...
Ha Ha Ha Ha Ha Ha Ha
P.S. Have a nice day.
Ha Ha Ha Ha Ha Ha Ha
(Click to continue...)

USERS SHOULD NOT POWER DOWN THE SYSTEM IF THEY SEE THIS MESSAGE.
Powering down the system can corrupt the disk, leading to possible serious damage.

Name: CODE-1		
Aliases: CODE-1, CODE 1	**Type:** Bogus CODE resource.	
Disk Location: Application programs and Finder.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Renames Hard disk	**Size:** CODE	**See Also:**

Notes: Virus: CODE-1
Damage: Alters applications and system file; may rename hard disk; may crash system or damage some files. See below.
Spread: possibly limited, but has potential to spread quickly
Systems affected: All Apple Macintosh computers, under Systems 6 & 7.

Several sites have reported instances of a new Macintosh virus on their systems. This virus spreads to application programs and the system file. Its only explicit action, other than spreading, is to rename the hard disk to "Trent Saburo" if the system is restarted on October 31 of any year. However, the virus changes several internal code pointers that may be set by various extensions and updates. This may lead to system failures, failures of applications to run correctly, and other problems. Under some conditions the virus may cause the system to crash.

The virus detected by some virus protection programs on some Macintosh machines (but no anti-virus program released prior to this date specifically recognizes this virus). This behavior depends on the nature of the hardware and software configuration of the infected machine.

Name: Conan the Librarian		
Aliases: Conan the Librarian	**Type:** Joke program, not a virus.	
Disk Location: Startup Item	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This applications monitors ambient noise from the Macintosh microphone. If noise crosses certain threshhold, a voice with Austrian accent asks for quiet. As noise continues, voice gets more firm and finally shouts "shut up!" To remove, restart with extensions off and remove from Startup Items folder.		

Name: CPro 1.41.sea		
Aliases: CPro 1.41.sea, CompacterPro, log jingle	**Type:** Trojan.	
Disk Location: CPro 1.41.sea program	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: CPro 1.41.sea appears to be a self extracting archive containing a new version of Compactor Pro. When run, it reformats any disk in floppy drive 1, and attempts (unsuccessfully) to format the boot disk. The program contains a 312 byte snd resource named "log jingle" containing a sound clip from the Ren and Stimpy cartoon series. Formats floppy disk in drive 1 File named CPro 1.41.sea Contains:312 byte snd resource named "log jingle" All current utilities		

Name: Dimwit		
Aliases: Dimwit	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Dimwit causes the Mac screen to dim to 25% of its brightness over the course of about 5 minutes. Depressing the CAPS LOCK key resumes it's original brightness until the key is unlocked. To remove, remove it from the System (Extensions) Folder and restart.		

Name: DOS sHELL		
Aliases: DOS sHELL	**Type:** Joke program, not a virus.	
Disk Location: "System Extension"	**Features:**	
Damage: "Does no damage."	**Size:**	**See Also:**
Notes: Replaces the "Welcome to Macintosh" startup to a DOS shell prompt. Clicking any key displays the programmers name; clicking again resumes the normal startup. Remove by removing from system extensions folder.		

Name: Dukakis		
Aliases: Dukakis	**Type:** Program.	
Disk Location: Hypercard stack.NEWAPP.STK stack	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:**	**See Also:**
Notes: Written in HyperTalk on a HyperCard stack called "NEWAPP.STK". Adds itself to Home Card and other stacks. Flashes a message saying, "Dukakis for President in 88, Peace on Earth, and have a nice day." This virus can be eliminated by using the Hypertalk editor and removing the well commented virus code.		

Name: Enchanted Menus		
Aliases: Enchanted Menus	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Causes menus selected from menu bar to pop up in random places instead of directly beneath the bar. To remove, remove it from the System (Extensions) Folder and restart.		

Name: FlyPaper		
Aliases: FlyPaper	**Type:** Joke program, not a virus.	
Disk Location: Startup Item	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: FlyPaper causes the desktop to get dragged with the cursor. The CAPS LOCK or loud noise (on Microphone equipped Macs) exits the program. To remove, restart with extensions off and remove from system startup items folder (System 7) or locate and trash it (System 6).		

Name: FontFinder Trojan		
Aliases: FontFinder Trojan	**Type:** Trojan.	
Disk Location: FontFinder program	**Features:**	
Damage: Corrupts a program or overlay files.Corrupts a data file.Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: Trojan found in the Public Domain program called 'FontFinder'. Before Feb. 10, 1990, the application simply displays a list of the fonts and point sizes in the System file. After that date, it immediately destroys the directories of all available physically unlocked hard and floppy disks, including the one it resides on. VirusDetective search string: Filetype=APPL & Resource Start & WData 4E76#84EBA#E30#76702 ; For finding Mosaic/FontFinder Trojans		

Name: Hal		
Aliases: Hal	**Type:** Joke program, not a virus.	
Disk Location: System ExtensionApplication programs and Finder.	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This application generates extension(s) that cause predetermined strings to be substituted when typed in. For example, one may be created to substitute "Dumb Operating Syetem" when the user types DOS. There is one extension per substitution string. To remove, the extensions have to be removed from the Startup (system 6) or startup extensions folder.		

Name: HC		
Aliases: HC, HyperCard virus	**Type:** Program; activates when run.	
Disk Location: HyperCard Stacks	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Sam 3.o search def: Virus Name: HC Virus File Type: STAK Search String pop-up menu: ASCII Search String text field: if char 1 to 2 of LookAtDate <11 The string in the Search String text field above is an ASCII string. Blank area between words are spaces. The string IS case sensitive. As a guard against incorrect entry, SAM 3.0 has a "Check field" in the Definitions dialog boxes. If all of the above information is entered correctly, then your check field should be A0BD.		

Name: HC-9507		
Aliases: HC-9507, HC 9507	**Type:** Program.	
Disk Location: Hypercard stack.	**Features:**	
Damage: No damage, only replicates.	**Size:**	**See Also:**

Notes: 31 July 1995

Virus: HC-9507
Damage: Infects HyperCard stacks only; does not infect system files or applications.
Spread: Once the home stack is infected, the virus spreads to other running HyperCard stacks and other randomly chosen stacks on the startup disk.
Systems affected: All Apple Macintosh computers, under Systems 6 & 7.

The HC-9507 virus causes unusual system behaviors, depending on the day of the week and the time. While running HyperCard with infected stacks, you may observe the screen fading in and out, the word "pickle" being entered automatically, or your system may suffer a shutdown or lockup.

According to feedback from the publishers and authors of the major anti-viral software programs, information about upgrades to known, actively supported Mac anti-virus products is as follows:

Tool: SAM (Virus Clinic and Intercept)
Status: Commercial software
Revision to be released: 4.0.5

Tool: Virex
Status: Commercial software
Revision to be released: A free virus definition will be made available for all versions of Virex 5.5 or later immediately. This definition will be built into versions 5.5.5 and later.

Other antivirals:
CPAV (Central Point Anti-virus) does not normally deal with HyperCard viruses, so no update is needed.
Disinfectant does not deal with HyperCard viruses, so no update is needed.
Gatekeeper is no longer actively supported. However, its design is such that no update would be needed.
No information is available at this time about the "Rival" antivirus program and this virus.
VirusDetective is not supported against HyperCard viruses so no update is needed.

Name: Hermes Optimizer 1.1		
Aliases: Hermes Optimizer 1.1	**Type:** Trojan.	
Disk Location: Hermes Optimizer 1.1 program	**Features:**	
Damage: Deletes or moves files.Renames files.	**Size:**	**See Also:**

Notes: The Hermes Optimizer 1.1 Stack is supposed to decrease the level of fragmentation in a HermesShared file. It is actually a Trojan Horse program that renames all files on your hard disk, moves them and then deletes them. You can recover the files with most standard utiltiies, but must go through each one, one at a time to figure out what it is and where it belongs. No files left on your disk. You find a stack with the name Hermes Optimizer 1.1 Don't run the Hermes Optimizer 1.1 stack, dump it in the trash. Recover any lost files with standard file utilities like those supplied with Norton Utilities or Central Point's MacTools. Check each file individually to see what it's name is and where it belongs.

Name:INIT 1984		
Aliases: INIT 1984, INIT1984	**Type:** Bogus INIT.	
Disk Location: INIT program.	**Features:**	
Damage: Deletes files.Modifies names & attribs of files and folders	**Size:** INIT # 1984 added to system folder.	**See Also:**
Notes: Infects system extensions of type "INIT" (startup documents). Does NOT infect the System file, desktop files, control panel files, applications, or document files. As INIT files are shared less frequently than are applications, and also due to the way the virus was written, this virus does not spread very rapidly. There have been very few confirmed sightings of this virus as of 3/17/92. (incl one in Netherlands and 1 in NYState). Virus works on both System 6 and System 7. Damage only occurs when system is BOOTED on Friday the 13th, after 1991. On old Mac's with 64K ROMs, it will crash. Gatekeeper and SAM Intercept, in advanced and custom mode were able to detect this virus's spread. on any Friday the 13th in any year 1991 and above, will trigger. Damage includes changing names and attributes of folders&files to random strings, and deletion of less than two percent of files		

Name:INIT-17		
Aliases: INIT-17, INIT17	**Type:** Bogus INIT.	
Disk Location: Application programs and Finder.System program.	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** INIT #17 added to files.	**See Also:**
Notes: The virus is to display an alert message in a window entitled "From the depths of Cyberspace" the first time an infected machine is rebooted after 6:06:06 pm, 31 Oct 1993. Lots of bugs in this virus cause earlier Macs to crash.		

Name:INIT-M		
Aliases: INIT-M	**Type:** Bogus CODE resource.	
Disk Location: Applications and the Finder	**Features:**	
Damage: Corrupts a program or overlay files.Corrupts a data file.Deletes or moves files.	**Size:** CODE	**See Also:**
Notes: INIT-M rapidly spreads only under System 7; it does not spread or activate on System 6 systems. The virus activates on any system running on Friday the 13th, files and folders will be renamed to random strings, creation and modification dates, and file creator and type information will be changed, files will be deleted. Recovery from this damage will be very difficult or impossible. The file "FSV Prefs" will be found in the Preferences file. Delete infected files		

Name:INIT29		
Aliases: INIT29	**Type:** Bogus INIT.	
Disk Location: Application programs and Finder.Document file.INIT program.	**Features:**	
Damage: Corrupts a program or overlay files.Interferes with a running application.Corrupts a data file.	**Size:** INIT ID#29	**See Also:**
Notes: It infects any file with resources, including documents. It damages files with legitimate INIT#29 resources. If you see the following alert whenever you insert a locked floppy, it is a good indication that your system is infected by INIT 29. The disk "xxxxx" needs minor repairs. Do you want to repair it? Also, printing problems and unexplained crashes If you find an INIT ID=29 on an application or the System file, you may have this virus. There are two Virus Detective search strings, one for the Finder and Applications, and one for nonapplications: Resource Start & Size<800 & WData 41FA#92E#797 ; For finding INIT29 in Appl's/Finder Filetype≠APPL & Resource INIT & Size<800 & WData 41FA#92E#797 ; For finding INIT29 in non-Appl's Removing the INIT repairs the files.		

Name: MacBarf		
Aliases: MacBarf	**Type:** Joke program, not a virus.	
Disk Location: Control Panel	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Mac plays vomiting sound whenever a diskette is ejected. To remove, remove it from the System (Control Panels) folder and restart.		

Name:MBDF A		
Aliases: MBDF A	**Type:** Bogus resource. MBDF	
Disk Location: Applications and the FinderTETRICYCLE TrojanTetris-rotating Trojan	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** Modifies CODE #0, adds 630 bytes to infected files	**See Also:** MBDF, MBDF-B
Notes: March 4, 1992: Correction: it DOES spread on ALL types of macintoshes if the operating system is System 7. It will not spread on a MacPlus or SE if that system is using System 6.x Virus has to rewrite System file to infect it, can take up to 3 mins, if interrupted (think it hung) will destroy system and would have to reload all of it. Does NOT affect data files. Does not do malicious damage. 2 Cornell students have been accused of releasing it on Feb 14, 1992 to archive sites. The file TETRICYCLE (also named "Tetris-rotating) is a trojan which installs the virus, the first anti-viral updates did not locate this virus. See also below for more details. SAM's old version knows something was up (when it was installed with all options on) , but it would give an alert and not allow the option to push the DENY button Disinfectant 2.6, Gatekeeper 1.2.4, Virex 3.6, SAM 3.0, VirusDetective 5.0.2, Rival 1.1.10 Claris applications will note code change, old ver. SAM running full tilt will also detect. Anti-viral products mentioned above		

Name: MBDF-B		
Aliases: MBDF-B, MBDF B	**Type:** Bogus resource. MBDF	
Disk Location: Application programs and Finder.	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** Modifies CODE #0, adds 630 bytes to infected files	**See Also:** MBDF-A

Notes: Virus: MBDF-B
Damage: minimal, but see below
Spread: probably limited
Systems affected: Apple Macintosh computers. The virus spreads on all types of Macs except MacPlus systems and (perhaps) SE systems; it may be present on MacPlus and SE systems and not spread, however.

A new variant of the MBDF-A virus has recently been discovered. It seems that a person or persons unknown has modified the original MBDF-A virus slightly and released it. Like the original, this virus does not intentionally cause damage, but it may spread widely.

The virus does not necessarily exhibit any symptoms on infected systems. Some abnormal behavior has been reported in machines infected with MBDF-A, involving system crashes and malfunctions in various programs, which may possibly be traced to the virus. Some specific symptoms include:

* Infected Claris applications will indicate that they have been altered
* The "BeHierarchic" shareware program ceases to work correctly.
* Some programs will crash if something in the menu bar is selected with the mouse.

The MBDF-B virus should behave similarly and will spread under both System 6 and System 7.

Name: MDEF		
Aliases: MDEF, MDEF A, Garfield, MDEF B, Top Cat, MDEF C	**Type:** Bogus resource. MBDF	
Disk Location: System program.Application programs and Finder.Desktop file.Document file.	**Features:**	
Damage: Interferes with a running application.	**Size:** MDEF ID#0	**See Also:**

Notes: MDEF infects applications, the System file, other system files, and Finder Desktop files. The System file is infected as soon as an infected application is run. Other applications become infected as soon as they are run on an infected system. MDEF's only purpose is to spread itself, and does not intentionally attempt to do any damage, yet it can be harmful. Odd menu behavior. VirusDetective search string: Resource MDEF & ID=0 & WData 4D44#A6616#64546#6A9AB ; For finding MDEF A & MDEF B
SAM def: Name=Garfield, Resource type=MDEF, Resource ID=0, Resource Size=314, Search String=2F3C434F44454267A9A0, String Offset=42
SAM def: Name=GARFIELD-2, Resource type=MDEF, Resource ID=0, Resource Size=532, Search String=2F3C4D4445464267487A, String Offset=304
SAM def: Name=MDEF C, Resource type=MDEF, Resource ID=0, Resource Size=556, Search String=4D4445464267487A005EA9AB, String Offset=448

Name: MenuHack		
Aliases: MenuHack	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**

Notes: MenuHack causes the menus in the menu bar to switch places when the user attempts to select.
To remove, remove from System Extensions folder and restart.

Name: merryxmas		
Aliases: merryxmas, Merry Xmas	**Type:** Program.	
Disk Location: Hypercard stack.	**Features:** Direct acting.	
Damage: No damage, only replicates.Can cause Hypercard to quit	**Size:** 0 to 1 file allocation block	**See Also:**

Notes: Analysis of the Macintosh Merry Xmas virus 11/3/93
W. J. Orvis

Type: Program virus in a Hypercard script
Infection: Infects all open, unlockable stacks by copying itself to the end of the stack script.
Damage: None intentional
Size: 0 to 1 allocation block since it adds to the end of the stack script, and the stack script is increased by an allocation block whenever the script extends passed the end of the current block.

Disinfection: Open hypercard, switch to the last card in the home stack and set it to scripting. Open the infected stack select Objects Stack Info and click Script. Find the virus at the end of the script and delete it. To make it so SAM won't detect it, type enough characters to overwrite the script, save it, then delete the typed characters and save it again. Check the stack script on your home stack to see if it was infected while you were disinfecting the infected stack.

When the virus is active, the disk is continually accessed by an 'on idle' procedure, even though it is not infecting the stack. If the stack is from Hypercard version 1, the virus can not infect it because it can not be unprotected. If the stack is converted to version 2, the virus can unprotect and infect it.

SAM with the 4/27/93 virus definitions will see this virus. If the virus has simply been deleted, the virus key will still be in the stack beyond the EOF for the stack script causing SAM to detect the virus in a disinfected stack. The virus inserts itself by counting off a number of lines from the bottom of the stack, so adding lines to the virus will mess it up.

Name: Minitors		
Aliases: Minitors	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**

Notes: Minitor decreases the size of the monitor display by one pixel each startup.
It maintains the screen's proportions and moves the finder icons in.
To remove, remove it from the system extensions folder. If you have reached the point where the
Mac crashes (just enough for the menu bar), restart without extensions and then remove.

Name: Mitten Touch-Typist		
Aliases: Mitten Touch-Typist	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**

Notes: Generates random keystroke errors; approximately one per 15 characters types.
Program automatically stops loading after three system boots; to permanently remove, remove it from the System (System6) or System Extensions (System 7) folder.

Name: Moof		
Aliases: Moof	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Moof causes all text displayed on the Mac to be "Moof" with the o's streching it out to the length of the original word. To remove, remove it from the Systems Folder by identifying the icon with the "Dogcow". Then resart the computer. Restart is in the special menu which is the second from the right on System 6 and the last on System 7. Restart is the second menu item from the bottom (on Powerbooks, the third). Look for items with the same number of characters.		

Name: Mosaic Trojan		
Aliases: Mosaic Trojan	**Type:** Trojan.	
Disk Location: Mosaic program	**Features:**	
Damage: Corrupts a program or overlay files.Corrupts a data file.Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: Imbedded in a program called 'Mosaic', when launched, it immediately destroys the directories of all available physically unlocked hard and floppy disks, including the one it resides on. The attacked disks are renamed 'Gotcha!'. VirusDetective search string: Filetype=APPL & Resource Start & WData 4E76#84EBA#E30#76702 ; For finding Mosaic/FontFinder Trojans		

Name: Munch		
Aliases: Munch	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Munch causes large "bites" to be taken out of windows and display boxes. Uneaten portions are still usable. After finishing, the Mac emits a loud burp and smacking noises, and resumes on any new windows that are displayed. To remove, remove from System (Extensions) Folder and restart.		

Name: NetDino StartDino		
Aliases: NetDino StartDino	**Type:** Joke program, not a virus.	
Disk Location: System ExtensionApplication programs and Finder.	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: NetDino causes a small dinosaur to move across the screen of the Mac, and then to move onto the screen of another Mac in the Network. StartDino is an application for managing what networked machines the dinosaur visits. Holding the mouse button as the dinosaur leaves a screen stops the action. To remove, remove from the System (Extensions) Folder of each infected Mac and restart.		

Name: nVIR		
Aliases: nVIR, nVIR A, nVIR B, AIDS, Hpat, MEV#, FLU, Jude, J-nVIR	**Type:** Patched CODE resource.	
Disk Location: Application programs and Finder.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** nVIR In system ID #0,1,4,5,6,7; In application ID#1,2,3,6,7CODE In applciation ID#256INIT In system ID#32Hpat, MEV#,AIDS,FLU Varations of nVIR resource name in other mutations	**See Also:**
Notes: It infects the System file and applications. nVIR begins spreading to other applications immediately. Whenever a new application is run, it is infected. Symptoms include unexplained crashes and problems printing. Works on Atari ST's in MAC emualtion mode. Unexplained system crashes, problems printing. There are two Virus Detective search strings, one for applications and one for the System file: "Resource Start & Size<800 & WData 2F3A#F00#C80#B00 ; For finding nVIR, etc. in Appl's/Finder" "Filetype=ZSYS & Resource INIT & Size<800 & WData 2F3A#F00#C80#B00 ; For finding nVIR, etc. (System)"		

Name: NVwls		
Aliases: NVwls	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This extension prevents the user from being able to input vowells at the keyboard. To remove, remove it from the System folder (System 6) or System Extensions folder (System 7) and restart.		

Name: Off Hook		
Aliases: Off Hook	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This extensions causes the Mac to simulate a telephone that has been off the hook. This includes voice warning messages and the Beep-beep-beep for 15 seconds. To remove remove it from the Systems extensions folder and restart.		

Name: Peace		
Aliases: Peace, MacMag virus, Drew, Brandow, Aldus	**Type:** Bogus INIT.	
Disk Location: Hypercard stack.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** INIT ID#6 on System	**See Also:**
Notes: First virus on the Macintosh. Displays "Peace on Earth" message on March 2, 1988 and removes itself the next day. Distributed via a HyperCard stack. Its presence causes problems with some programs. Rumored that a writer for the current show "Star Trek: The Next Generation" wrote it and was being accused in court and being sued: this info came out in late 1992 Unexplained program crashes. "Peace on Earth" message on March 2, 1988 INIT number ?? found on system file. VirusDetective search string: "Resource INIT & Size<2000 & WData 494E#37A#86700 ; For finding Peace" SAM search string: "" Remove the INIT from the System File.		

Name: Playin' Possum		
Aliases: Playin' Possum	**Type:** Joke program, not a virus.	
Disk Location: Startup Item	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Plays "Taps" on a bugle and shuts down the Mac. To remove, restart Mac with extensions off (hold down shift key) and remove from Startup Items folder in System folder.		

Name: Radiation Trigger		
Aliases: Radiation Trigger	**Type:** Joke program, not a virus.	
Disk Location: System ExtensionApplication programs and Finder.	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This extension/application combination allows someone to generate phony alert boxes on a networked Mac. The extension, Radiation, is the received and must be installed on each Mac to display messages. Trigger is the sending application. Any click on the receiving Mac gets rid of the alert box. To remove, remove Radiation from the System (Extensions) Folder from each of the Macs. Note also that Program Linking must be enabled for Guests in the Users & Groups Control Panel. If this is not your default setting, use the control panel to turn the program linking privilege off for guests.		

Name: Scores		
Aliases: Scores, NASA	**Type:** Patched CODE resource.	
Disk Location: Application program.System program.	**Features:**	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** INIT ID#6, 10, and 15 on the System, Notepad, Desktop, and Scrapbook filesatpl ID#128 on systemDATA ID#400 on the SystemCODE ID# n+1 on applications, n is the first unused CODE resource ID.	**See Also:**
Notes: Infects applications and the system, and attempts to destroy files with creator types: VULT, and ERIC. Causes problems with other programs, including unexplained crashes and pronting errors. Changes the icons of the NotePad and Scrapbook files to the blank document icon. Check the icons for the Note Pad and Scrapbook files. They should look like little Macintoshes. If they both look like blank sheets of paper with turned-down corners, your software may have been infected by Scores There are two Virus Detective search strings, one for the Finder and Applications, and one for the System file: Resource Start & Size<8000 & WData FD38#FBA#5A3 ; For finding Scores in Appl's/Finder Filetype≠APPL & Resource INIT & Size<1100 & WData FD38#FBA#5A3 ; For finding Scores in System, etc.		

Name: Sexplosion		
Aliases: Sexplosion	**Type:** Joke program, not a virus.	
Disk Location: Application programs and Finder.	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: The application has a suggestive title and a female icon. If a curious user executes it, a system bomb alert box appears with a highlighted Restart button and dimmed Resume button. When trying to click on the Restart button, it moves out of the way. The actual way to quit is to click on the dimmed Resume button. This is an application and may appear anywhere on the system.		

Name: Sexy Ladies Trojan		
Aliases: Sexy Ladies Trojan	**Type:** Trojan.	
Disk Location: Sexy Ladies application	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: Not a virus, but a Trojan Horse. Given away at 1988 San Fransisco MacWorld Expo, erased whatever hard disk or floppy disk it was on when it was lanched. An application named Sexy Ladies that erases the disk that contains it. Presence of the Application Sexy Ladies Delete the application		

Name: Sneezomatic		
Aliases: Sneezomatic	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Sneezomatic prevents the mounting of floppy diskettes. Whenever a diskette is inserted, it is ejected with an accompanying sneezing sound. To remove, remove it from the System (Extensions) Folder and restart.		

Name: Sniff		
Aliases: Sniff	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Plays "cold" sounds randomly at 15 second to 3 minute intervals. Sounds including sniffling, throat clearing, and coughing. To remove, remove it from the System (Extensions) Folder and restart.		

Name: Solvent		
Aliases: Solvent, Li'l Devil	**Type:** Joke program, not a virus.	
Disk Location: Startup Item	**Features:**	
Damage: Does no damage.	**Size:** Adds File	**See Also:**
Notes: Solvent causes the desktop to distort and melt until mouse button is clicked. It is installed as a startup item (System 7) or from Finder set startup (System 6). It may be renamed to make it difficult to find. To remove, restart with extensions off and copy program to trash. If starting with extensions off does not prevent Solvent from starting, start the Mac with the mouse button pressed. Then locate and trash the file.		

Name: Sonic Boom		
Aliases: Sonic Boom	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: The Mac makes glass breaking sound and and makes the screen look shattered whenever the Mac would normally emit a system beep, such as clicking outside a dialog box. To remove, remove it from the System (Extensions) Folder and restart.		

Name: Sproing		
Aliases: Sproing	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This extension causes the cursor to overshoot its mark and bounce back and forth until settling on a spot, such as if it were attached to a spring. Depressing the CAPS LOCK disables this action. To remove, remove from the System (Extensions) Folder and restart.		

Name: Squeaker		
Aliases: Squeaker	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Squeaker causes the Mac to emit squeak everytime mouse button is pressed. To remove, remove it from System (Extensions) Folder and restart.		

Name: StartupScreen Broken Mac Out of Order Melting Mac		
Aliases: StartupScreen Broken Mac Out of Order Melting Mac	**Type:** Joke program, not a virus.	
Disk Location: System program.	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: The "Welcome to Macintosh" startup screen is easily replaced by a PICT file named StartupScreen in the system folder. Two files from The Macintosh Joker, "Broken Mac" and "Melting Mac" may be used as the startup screen, as well as in others. To remove, move the StartupScreen file out of the system folder.		

Name: Steroid Trojan		
Aliases: Steroid Trojan	**Type:** Trojan.	
Disk Location: Steroid INIT programINIT program.	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:** Steroid INIT inserted in the System Folder.	**See Also:**
Notes: The steroid INIT is claimed to speed up QuickDraw on Macintoshes with 9 inch screens. The INIT has code that checks for dates after June 30, 1989, and is active every year thereafter from July through December. When it is activated, it attempts to erase all mounted drives. All mounted drives are erased. You may be able to save them with a disk editor like SUM or MacTools. Find the Steroid INIT in the System file VirusDetective search string: Resource INIT & Size<1200 & WData FE680C6E#E4EBA#F60 ; For finding Steroid Trojan SAM def: Name=Steroid Trojan, Resource type=INIT, Resource ID=148, Resource Size=1080, Search String=ADE9343C000A4EFAFFF24A78, String Offset=96 Remove the Steroid INIT from the System file.		

Name: T4		
Aliases: T4, T4-A, T4-B, GoMoku, T4-C	**Type:** Program; activates when run.	
Disk Location: Applications and the FinderGoMoku versions 2.0 and 2.1	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Damages system file	**Size:**	**See Also:**
Notes: The T4 virus was discovered in the game GoMoku versions 2.0 (T4-A) and 2.1 (T4-B). The name of the person in the game is not the virus author. The virus infects applications and the Finder, and attempts to alter the system file. Infected applications can not be fixed. The altered system file may not boot, or may not load INITS. The virus masquerades as Disinfectant to try to bypass protection software such as GateKeeper. Once installed, the virus does not seem to do any overt damage. INITs don't load. Alerts that disinfectant is changing a file when Disinfectant is not running indicates the virus is present. System Won't boot. Use a virus checking program Replace applications and reinstall the System and Finder. The applications, System, and Finder can not be repaired.		

Name: Termites		
Aliases: Termites	**Type:** Joke program, not a virus.	
Disk Location: Control Panel	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: This program makes it appear as if tiny termites are eating their way through everything on the screen. Everything works O.K., but it gets increasingly difficult to read the screen. To remove, remove from the System (Control Panels) Folder and restart.		

Name: Tweety		
Aliases: Tweety	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Mac plays random bird sounds. To remove, remove it from the System (Extensions) Folder and restart.		

Name: Umlaut Omelette		
Aliases: Umlaut Omelette	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: Umlaut Omelette causes the Mac text to be displayed with randomly generated diacritical and circumflex marks over every vowell. To remove, remove it from the System (extensions) folder and restart.		

Name: Vanish		
Aliases: Vanish	**Type:** Joke program, not a virus.	
Disk Location: System Extension	**Features:**	
Damage: Does no damage.	**Size:**	**See Also:**
Notes: The Vanish extension causes the Mac to not display text, including menus, title bars, and folder names. To remove, remove the Vanish application from the system extensions folder, identifying it by its icon of a letter being erased. Then restart the computer. This can be done by finding the last pull down menu, (second to last on System 6) in the title bar. The restart is second from the bottom (third on PowerBooks).		

Name: Virus Info Trojan		
Aliases: Virus Info Trojan	**Type:** Trojan.	
Disk Location: Virus Info Program	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This application has not been sighted outside of the Edmonton, Province of Alberta, Canada area where it was discovered. When activated, destroys the directory structure VirusDetective search string: Filetype=APPL & dataFork & Size < 10000 & WData A003#24E94 ; For finding Virus Info Trojan		

Name: WDEF		
Aliases: WDEF, WDEF-A, WDEF-B	**Type:** Bogus resource. WDEF	
Disk Location: Desktop file.	**Features:**	
Damage:	**Size:** WDEF ID = 0 in Desktip file	**See Also:** CDEF

Notes: WDEF only infects the invisible "Desktop" files used by the Finder. It can spread as soon as a disk is inserted into a machine. An application need not be run to cause infection.

Does not infect System 7 and above versions of the operating system due to changes in the O/S

VirusDetective search string: Creator=ERIK & Executables ; For finding executables in the Desktop

Find WDEF ID=0 in the Desktop file. Rebuild the Desktop - Hold down Command and Option while inserting the disk.

Name: Winnie the Pooh		
Aliases: Winnie the Pooh	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: We don't know if this is real. None of us has heard of it before, but the original information came off of AppleLink. We also don't know of an "older virus" with these characteristics.

There is an older virus that is resurfacing specifically with the High Volume computers. When a disk is inserted a dialog box pops up with an icon of Winnie the Pooh and the message "This disk is totally ------ up. Fix it?" and then the buttons "Yea" or "No Way

The second possible message is "This disk has been erased" there is an "OK button that when clicked gives the message "Haha ---head!

Name: ZUC		
Aliases: ZUC, ZUC 1, ZUC 2	**Type:** Patched CODE resource.	
Disk Location: Application programs and Finder.	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: It infects only applications files. Before March 2, 1990 or less than two weeks after an application becomes infected, it only spreads from application to application. After that time, approximately 90 seconds after an infected application is run, the cursor begins to behave unusually whenever the mouse button is held down. The cursor moves diagonally across the screen, changing direction and bouncing like a billiard ball whenever it reaches any of the four sides of the screen. The cursor stops moving when the mouse button is released. Wild shifts in cursor position.

Changes in the background pattern VirusDetective search string: Filetype=APPL & Resource CODE & ID=1 & WData A746*A038#31E*A033; For finding ZUC.Virus 1&2

SAM def: Name=ZUC A, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=4E56FF74A03641FA04D25290, String Offset=any

SAM def: Name=ZUC B, Resource type=CODE, Resource ID=1, Resource Size=any, Search String=7002A2604E752014A0552240, String Offset=any

MS-DOS/PC-DOS Computer Virus Table

Name: 10 past 3			
Aliases: 10 past 3	**Type:** Program.		
Disk Location: COM application.COMMAND.COM.		**Features:** Memory resident; TSR.	
Damage:		**Size:** 748	**See Also:**
Notes:			

Name: 1024PrScr			
Aliases: 1024PrScr, 1024, PrSc, PrScr	**Type:** Program.		
Disk Location: COM application.COMMAND.COM.		**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.		**Size:** 1024	**See Also:**
Notes: This virus will occasionally produce a "Print Screen" effect.			

Name: 109 Virus			
Aliases: 109 Virus	**Type:** Program.		
Disk Location: COM application.		**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.		**Size:**	**See Also:**
Notes: 1st discovered January 1992, this virus is a non-resident, direct action .COM file infector. It contains no text or payload and is a simple, yet effective replicater When an infected program is executed, it infects all .COM files in the current directory that meet the following conidions, adding 109 bytes. a. the file must be a .com file, filesize between 2 bytes and 64 kb. b. if the 1st bytre is BEh, assume that the file is already infected and do next file c. the file must have normal attributes, so if it is hidden or read-only, virus won't infect No error handling is done, the file time and date stamps will be changed upon infection It may damage a program larger than 65427 bytes, for the end of the infected program will be lost. hex string: BE 00 01 56 8C C8 80 C4 10 8E C0 33 FF			

Name: 12-TRICKS Trojan		
Aliases: 12-TRICKS Trojan, Twelve Tricks Trojan, Tricks	**Type:** Trojan.	
Disk Location: CORETEST.COMHard disk boot sectors.	**Features:**	
Damage: Corrupts the file linkages or the FAT.Attempts to format the disk.Interferes with a running application.Corrupts boot sector	**Size:**	**See Also:**
Notes: Contained in "CORETEST.COM", a file that tests the speed of a hard disk. It installs itself in the boot sector of the hard disk. Every time the computer boots, one entry in the FAT will be changed. With a probability of 1/4096, the hard disk will be formatted (Track 0, Head 1, Sector 1, 1 Sector) followed by the message: "SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC, 2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420". The following printed on the screen: "SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC,2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420" Damaged FATs and directories. All sorts of strange changes to typed or printed characters. Strange things happening when keys are typed. Text within the program CORETEST.COM, readable with HexDump-utilities:"MEMORY$" Text within the boot sector of the hard disk:"SOFTLoK+ V3.0 SOFTGUARD SYSTEMS,INC,2840 St.Thomas Expwy,suite 201, Santa Clara,CA 95051 (408)970-9420"		

Name: 1226		
Aliases: 1226, 1226D, 1226M, V1226, V1226D, V1226DM, (Phoenix related)	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: 1260		
Aliases: 1260, V2P1, Variable, Chameleon, Camouflage, Stealth	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** EncryptedDirect acting.Polymorphic	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 1260Polymorphic: each infection different	**See Also:** Vienna
Notes: This appears to be related to the Vienna virus. The virus infects any COM file in the current directory. Uses variable encryption techniques The seconds field of the timestamp of any infected program will be 62 seconds.		

Name: 1701		
Aliases: 1701, Cascade, Cascade B, Autumn, Herbst	**Type:** Program.Memory resident.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1701	**See Also:**
Notes: A variation of the 1704 (Autumn) virus. Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks.		

Name: 1704-Format		
Aliases: 1704-Format, Cascade Format	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedStealthDirect acting.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Attempts to format the disk.	**Size:** 1704	**See Also:**
Notes: Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks.		

Name: 2387		
Aliases: 2387	**Type:** Boot sector.	
Disk Location: COM application.EXE application.Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Corrupts a program or overlay files.Corrupts boot sector	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Polymorphic multi-partite fast infector Trigger: some time after it has been loaded in memory, it displays a rough fractal image using text mode and pseudo-graphic characters (it's hard to get this picture to come up) To spread, it infects the MBSector. When you boot from an infected HD, it infects EXE files as you execute them. PC's without a hard disk are immune.		

Name: 2UP		
Aliases: 2UP	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.EncryptedStealthWritten in Assembler	
Damage: Corrupts a data file.Displays messages. Drops letters on the screen	**Size:** A 6000 byte long, parasitic virus program.Also, takes 18 kbyte from memory	**See Also:**

Notes: The following notes are extracted from VB, April 1995:

2UP virus has appeared in Russia. It is 6 kbyte long, and it is written in Assembler language. 2UP infects EXE and COM files.
Execution of an infected file transmits the virus to the system memory. The decryption routine takes control from the host program, it restore the virus body to its original form, then it passes control to the installation routine. The installation routine checks for a memory-resident copy. If it fails to identify itself in memory, then the virus starts to install itself. It allocates 18 kbyte of memory for its use and hooks to Int 22h handler which is Program Termination Address, then it returns control to the host program. After the program termination, the virus moves itself to the system memory employing Int 22h.

The virus infects EXE and COM files. In the case of COM files, it writes itself in front of the host file. In the case of EXE file, the virus inserts itself between the header and body of the host file and it modifies the header so that control is passed to the virus code. 2UP modifies the directory sector on disk, it writes its ID stamp in the file directory entry. The stamping is accomplished by writing the string ' 2UP(C)1994' into the reserved field of the directory entry. This is used to prevent multiple infection. In addition, the virus uses a second test for self-recognition, it compares the file beginning with 15 bytes of the virus code.

When new files are created on the system, the memory-resident copy checks their names before infecting them. The name is check against the text string ' AID COMMAND ANTI AV HOOK SOS TSAFE -V SCAN NC ' to avoid infecting any of the anti-virus programs, COMMAND.COM, etc.

2UP has several payloads and the payload may be delivered as soon as the virus gets control. While 2UP installs itself into the system memory, it calls Int 21h with AX=F66h, if register CX returns a value of 4F6Bh, then the following message is displayed: Hello BOBBY ! (BOBBY-Trash Soft & Hardware)
Also, the virus has several video effect messages. One video effect is triggered by the occurrence of an error ; It selects a line on the screen randomly and character will be raised from their places and dropped back to place. The second video effect is triggered under certain condition by either the execution of an anti-virus program or opening a file. This video effect covers the whole screen with 2UP and test strings related to virus. The proper conditions for this video effect are even--number months and the current second of 58 or 59.
Sometimes the virus overwrites newly created files with the second video message.

The recommended method for disinfection is to use clean system conditions, then identify and replace the infected files.

Name: 3APA3A		
Aliases: 3APA3A, Zaraza	**Type:** Multipartite.	
Disk Location: Floppy disk boot sector.IO.SYS of hard dick(	**Features:** Encrypted (in Russian)Memory resident; TSR.StealthPolymorphicInfects disk ≥ 16MB, only	
Damage: Deletes or moves files.Display message during August of any year.	**Size:** 1024 byte long, written in two 512 byte sectors.Adds the attribute " VOLUME " to IO.SYS on hard disk.	**See Also:**

Notes: The following notes are extracted from VB Nov. 1994.

This virus was cultivated in Russia, the word 3APA3A means " infection " in Russian and its pronounced "ZARAZA".
The text is encrypted in Russian, but Anglicized.It can be displayed using standard DOS display driver.

The virus code is 1024 byte long and consists of 512 sectors. The first sector contains the virus installation code and the floppy disk infection routines. The second part contains hard disk infection routine and it is placed on the boot sector of floppy disk!.

The virus is capable of recognizing itself on floppy disks and hard disk. On hard disk, it checks the first root directory entry for VOLUME attribute. On floppy disk, It looks to its own ID-byte (i.e. compares the byte at the offset 21h with the value of 2Eh).
The virus intercepts Int 13h.

Hard disks are infected when an infected floppy disk is loaded. The virus decrypts itself, then passes the controls to the second sector of the virus code which contains hard disk infection routine. This infection routine reads the first boot sector of the hard disk and checks its size. If the size is less than 16 MB, no infection occurs. Otherwise, it calculates the address of the first sector, reads it, then checks the attributes of the first entry. In DOS, this entry is the IO.SYS file. If VOLUME is not listed as one of the attributes, then the virus starts its infection process. ZARAZA places a copy of IO.SYS in 3rd entry but written to the last cluster of the hard disk. Then, it overwrites the first entry (the original IO.SYS) with its own routine and adds the VOLUME attributes. The result of this manipulation is that the virus resides in memory and it avoids detection.

The triggering mechanism is the system date. When loading from an infected disk, during the month of "AUGUST" , the following message is displayed:
B BOOT CEKTOPE - 3APA3A
The message means " There is an infection in the boot sector ".

Removal of the virus from a hard disk is difficult. The standard DOS utilities such as SYS, LABEL are not capable of removing the virus and reconstructing the root directory. The use of specialist software is recommended. A scanner with routines that checks files via absolute access must be used. A second method is using a sector editor to reverse the change and re-construct the original root directory.

Name: 3X3SHR		
Aliases: 3X3SHR	**Type:** Trojan.	
Disk Location: 3X3SHR.???	**Features:**	
Damage: Erases the Hard Disk.	**Size:** 78848 bytes 3X3SHR file	**See Also:**

Notes: *TROJAN* Time Bomb type trojan wipes the Hard Drive clean.

Name: 3y		
Aliases: 3y	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: 4-days		
Aliases: 4-days	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: 405		
Aliases: 405	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overwrites first 405 bytes of a .COM file.	**See Also:**
Notes: The virus spreads itself by overwriting the first 405 bytes of a .COM file. One file is infected each time an infected file is executed.		

Name: 4096		
Aliases: 4096, Century, Century Virus,100 Years Virus, Frodo, IDF, Stealth	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.Program overlay files.COMMAND.COM	**Features:** EncryptedDirect acting.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Corrupts a data file.Corrupts the file linkages or the FAT.	**Size:** 4096 bytes increase in length, but hidden from the DIR cmd.	**See Also:**
Notes: It infects both .COM or .EXE applications. It is nearly impossible to detect once it has been installed since it actively hides itself from the scanning packages. Whenever an application such as a scanner accesses an infected file, the virus disinfects it on the fly. DIR will also not show the change in length. virus-l, v5-063: tries to place a new boot sector over the orig. on Sept 21 but the code to do this is garbled, so the computer will hang. v6-084: Frodo can infect certain types of non-executable files Almost none. The computer will hang at a Get Dos Version call when the date is after 9/22 and before 1/1 of next year. virus-l, v5-063: report that this virus will Activate on Sept 21. Compare file lengths with DIR and a Disk editor like Norton utilities. If they differ by 4096 you have the virus. If the date of the file is 20XX (XX being the last 2 digits of the original date) then the file has probably been infected by the 4096 virus Copying a file to a file with a non-executable extension results in a disinfected file because the virus removes itself when the file is copyed by COMMAND.COM. A Do-it-yourself way: Infect system by running an infected file, ARC/ZIP/LHARC/ZOO all infected .COM and .EXE files, boot from uninfected floppy, and UNARC/UNZIP/LHARC E etc. all files. Pay special attention to disinfection of COMMAND.COM. v6-151: At least one anti-virus program can detect and remove Frodo (F, G, and H)		

Name: 4870 Overwriting		
Aliases: 4870 Overwriting	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 4870	**See Also:**
Notes: This virus infects programs by overwriting, and thus destroying them.		

Name: 4res		
Aliases: 4res	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: 512		
Aliases: 512, 512-A, 512-B, 512-C, 512-D	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: The virus hides in the first 512 bytes of free space in the last cluster of a .COM file. When RAM-Resident, it hides in the disk buffer space for code in order not to take-up memory. Files do not appear to change in length, because the virus removes itself on the fly when the file is accessed by another program. virus-l, v4-131 says that a variant of the 512 and Doom-II virus can put executable code into video memory. "666" at offset 509. A Do-it-yourself way: Infect system by running an infected file, ARC/ZIP/LHARC/ZOO all infected COM and EXE files, boot from uninfected floppy, and UNARC/UNZIP/LHARC E etc. all files. Pay special attention to disinfection of COMMAND.COM.		

Name: 66a		
Aliases: 66a	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 512	**See Also:**
Notes:		

Name: 99%		
Aliases: 99%, 99 percent	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Corrupts a data file.	**Size:** 821	**See Also:**
Notes: This virus may overwrite files with a small Trojan that displays a message which starts with the line "Het 99%-virus heeft toegeslagen."		

Name: Abbas		
Aliases: Abbas	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Abraxas		
Aliases: Abraxas	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 11711200	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Ada		
Aliases: Ada	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 2600	**See Also:**
Notes: Ada is a resident .COM file infector found in Argentina. The virus may interfere with the operation of the PC-cillin anti-virus program.		

Name: Adolf		
Aliases: Adolf	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 475	**See Also:**
Notes: Adolf is a resident, .COM file infector that contains the string Adolf Hitler.		

Name: Advent		
Aliases: Advent, 2761	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Interferes with a running application.	**Size:** 2761-2776 Bytes are appended on a paragraph boundary	**See Also:**
Notes: Spreads between .COM and .EXE files. Beginning on every "Advent"(the 4th Sunday before Christmas until Christmas eve), the virus displays after every "Advent Sunday" one more lit candle in a wreath of four, together with the string "Merry Christmas" and plays the melody of the German Christmas song "Oh Tannenbaum". By Christmas all four candles are lit. This happens until the end of December, whenever an infected file is run. If the environment variable "VIRUS=OFF" is set, the virus will not infect.		

Name:AIDS		
Aliases: AIDS, Hahaha, Taunt, VGA2CGA	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase	**See Also:**
Notes: It infects .COM files.		

Name: AIDS II		
Aliases: AIDS II, AIDS	**Type:** Trojan.	
Disk Location: AIDS Information Introductory Diskette	**Features:**	
Damage: Encrypts the file directory.	**Size:** Adds File REM#.EXE 146188 bytes (hidden file)Adds File AIDS.EXE 172562 bytes	**See Also:**

Notes: On Monday, 11th December 1989, several thousand diskettes named "AIDS Information Introductory Diskette Version 2.0" were mailed out containing a program that purported to give you information about AIDS. These diskettes actually contained a trojan that will encrypt the file names on your hard disk after booting your computer about 90 times. If you have installed this program, you should copy any important data files (no executables) and reformat your hard disk. All your file names are encrypted and the disk is full. In the root directory, files named: AIDS.EXE, AUTO.BAT, AUTOEXEC.BAK
Two hidden subdirectories called # and ######
The # subdirectory contains a readonly, hidden file called REM#.EXE.
The ###### subdirectory contains a hidden subdirectory called ######
The ###### subdirectory contains a hidden subdirectory called ######
The ###### subdirectory also contains a subdirectory called ERRORIN.THE, and five files named
____.__, _._, ___._, _._ and _.__
(where _ is the underline character, is the space character, and # is Ascii 255).
The minimum required to disable the virus is to remove the AUTOEXEC.BAT file that runs the program REM#.EXE and to remove all the hidden directories. This will not insure removal of the virus. It would be better backup any needed data files (no applications) and to do a low level format of the hard disk.
If the virus has already been activated, you can recover the encrypted file names using the table below in the summary, and then reformat the disk.

Name: AIDS II		
Aliases: AIDS II, AIDS-II	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 8064Adds File	**See Also:**

Notes: AIDS II is a companion virus. When activated, it creates .COM files with the same name as .EXE files. DOS will always execute the .COM file first, which is the virus. The virus then executes the .EXE file when it is finished.

Name: Aircop		
Aliases: Aircop	**Type:** Boot sector.	
Disk Location: Hard disk boot sectors.Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:**	**See Also:**

Notes: from a report in virus-l, v4-220:
Causes FPROT 2.01 to hang, while FPROT 1.15 sometimes says its cured (but it never is)
CLEAN 7.9v84 says "Virus cannot be safely removed from boot sector"
DOS/SYS says "Not able to SYS to .3L File System"
The virus may display Red State, Germ Offensive AIRCOP when booting with an infected disk.

Name: Akuku		
Aliases: Akuku, Metal Thunder, Copmpl	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 8898921111 - Copmpl variant	**See Also:**
Notes: Contains the string A kuku, "Nastepny komornik !! " The Copmpl variant contains the string. "Sorry, I'm copmpletly dead"		

Name: Alabama		
Aliases: Alabama, Alabama-B, Alabama.C	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** EncryptedDirect acting.	
Damage: Corrupts the file linkages or the FAT.Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1560	**See Also:**
Notes: The Alabama virus is a memory resident, encrypting, .EXE file infector. The virus contains the string, SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW. Box 1055 Tuscambia ALABAMA USA. which is displayed after an hour of use on an infected machine. It hooks Crtl-Alt-Del and fakes a reboot when they are pressed, staying in memory. On Fridays, it does strange things like executing different files from those you selected. The following text on the screen, SOFTWARE COPIES PROHIBITED BY INTERNATIONAL LAW. Box 1055 Tuscambia ALABAMA USA. Executing one file and having a different one start running. v6-151: At least one anti-virus program can detect and remove Alabama.C		

Name: Albania		
Aliases: Albania	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 429506575606	**See Also:**
Notes: The viruses contain the word "Albania".		

Name: Alex		
Aliases: Alex	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 368	**See Also:**
Notes:		

Name: Alexander		
Aliases: Alexander	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1951	**See Also:**

Notes: Alexander contains the following encrypted text:

Apa depistata in microprocesor !
Functionarea poate fi compromisa !
Se recomandaoprirea calculatorului.
citeva ore pentru uscare !
Alexander - Constanta, Romania.

Name: Ambulance Car		
Aliases: Ambulance Car, REDX, Red Cross, Ambulance.E	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 796 to .COM files	**See Also:**

Notes: When an infected application is run, the virus tries to find two .COM file victims which it randomly selects in the current directory or via the PATH variable in the environment. After some number of executions (110b), an ambulance car with a flashing light runs along the bottom of the screen accompanied by siren sounds. A flag is set, so the car will not run again until the next bootup.

An ambulance car running along the bottom of the screen accompanied by siren sounds. almost every anti virus program almost every anti virus program can find and eradicate it.

Name: Amoeba		
Aliases: Amoeba, 1392	**Type:** Program.Memory resident - TSR	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Machine can crash	**Size:** Every time attached to end of file, deletes a byte ofvirus initialization code	**See Also:**

Notes: The Amoeba virus attaches to infected files in the front and end of the file. Each time the virus attaches to the end of a file, it drops a byte from the front of the virus initialization code, thus eventually after a few generations this virus will become unusable, and the machine will crash.
When activated, the text "SMA Khetapunk - Nouvel Band A.M.O.E.B.A by Primesoft Inc." appears on the screen.
To prevent reinfection, it uses F3 interrupt vector, if the value is CDCD it figures it is resident and won't infect.
It was written with an unusual assembler. There is no trigger date, machine can crash.
DDI's Data Physician Plus!, V 3.0C Data Physician Plus! v3.0C

Name: Anarchy.9594		
Aliases: Anarchy.9594	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.EncryptedStealthPolymorphic	
Damage: Decreases system memory by 83 kbytesWhen triggered, display message and halt the computer	**Size:** Polymorphic: each infection different9594 byte long	**See Also:** Anarchy.2048

Notes:
The following notes are extracted from VB Feb. 1995:

The virus is not typical: It is about 9 times longer than any typical virus and it decreases system memory by 83 kbyte (1 kbyte is typical). Thus, it required more time to disassemble.

When an infected file is executed, control is passed to the virus code and the virus attempts to infect the system memory. The virus check the DOS version, if its lower than DOS 3.0, then control is returned to the host file. If condition are suitable, then it calls the the undocumented Int 2Fh function (Installation Check function) to ensure the availability of other DOS function. Next, it checks for a memory resident copy of itself using the Int 21h function. If there is an active copy, then control is passed to the host file, otherwise is installs itself in the memory. The virus check the size of system memory and if the its sufficient, then it decreases the memory by 83 kbyte and copies its code to that area. Later, it hooks Int 09h, Int 21h, and Int 28h for its use. The virus use Int 21h function for infection, stealth, and triggering routines. It uses Int 09h and Int 28h for delivering its payload.

The virus checks file name and extension. It infects all COM and EXE files with the exception of COMMAND.COM file. Anarchy distinguishes EXE and COM files. It encrypt itself with its own polymorphic routines. The encrypted code is appended to the end of host file, writes JMP VIRUS to the header. The JMP VIRUS code for COM files is different from EXE file. Then, the length of file is adjusted to its original value, thus the file appears unchanged. The virus attaches the text string ' UNFORGIVON' to the end of the file. Finally, it add 100 years to date stamp of the host file. This change in the date stamp and ' UNFORGIVON' are used by the virus to identify infected files and avoid duplication.

The memory resident copy keeps a record of all infected file, since it was activated. If the count reaches 48, the virus delivers its payload, which is displaying one of its four messages. The second action of the virus is that it emulates the shell of Norton Commander whenever the Alt_Minus keys are pressed (Minus key of the numerical keypad only).

Note: Files located on remote disks are not infected by the virus.

The suggested method for disinfection is to identify and remove all infected files. The file identification is trivial. A clean system should be used for all disinfection process.

Name: Andro		
Aliases: Andro	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Andromeda		
Aliases: Andromeda	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Andryushka		
Aliases: Andryushka, Andriyshka	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** Variable	**See Also:**
Notes:		

Name: Angarsk		
Aliases: Angarsk	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 238	**See Also:**
Notes:		

Name: Angelina		
Aliases: Angelina	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.Stealth	
Damage: No damage, only replicates.	**Size:** Reduces memory by 1 kbyte for itself.	**See Also:**

Notes:
The following notes are extracted from VB, May 1995:
Angelina is boot sector virus in the UK and worldwide. It is just another normal boot sector with no payload. It exists only to propagate. The virus is transmitted via booting from an infected disk.

A message is encoded in the virus, but never displayed :

Greeting for ANGELINA!!! /
by Garfield /
Zielona Gora

The last line of the message is the name of town in Poland and its means 'Green Hill' in Polish.

The recommended method for removal is using FDISK/MBR command under clean system conditions.

Name: Anna		
Aliases: Anna	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 742	**See Also:**

Notes: Anna is an encrypted virus, which contains the text:

[ANNA] Slartibartfast, ARCV NuKE the French
Have a Cool Yule from the ARcV
xCept Anna Jones
I hope you get run over by a Reindeer
Santas bringin' you a Bomb
All my Lurve - SLarTiBarTfAsT
(c) ARcV 1992 - England Raining Again

Name: Anthrax		
Aliases: Anthrax, Anthrax PT	**Type:** Boot sector. Program.	
Disk Location: COM application.EXE application.Floppy disk boot sector.Hard disk boot sector.	**Features:** Multipartite	
Damage: Trashes the hard disk	**Size:** 1024	**See Also:**
Notes: Infects both boot sectors and files. Trashes hard disks. MS-DOS 6's antivirus routine detects some, but not all infections by Anthrax. v6-137: this is a multipartite virus that infects COM and EXE files, and the MBR. Replace all infected files with clean copies, and clean the MBR (if infected) v6-141: "...Once on a computer, it acts as a non-resident virus and infects only the files on the first DOS partition. It never infects anything on diskettes. Even if you copy an infected file on a diskette and execute it from there on a clean machine, the virus will not infect that machine - it doesn't infect when the floppy disk motor is on. The only way to get infected by it is to download an infected file, or to copy an infected file on the hard disk and to execute it from there. The only known cases of this virus in the wild were caused by downloading an infected program from a BBS and executing it...."		

Name: Anti Pascal		
Aliases: Anti Pascal, Anti Pascal 529, Anti Pascal 605, AP 529, AP 605, C 605, V-605	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Deletes or moves files.Interferes with a running application.Corrupts a program or overlay files.	**Size:** 605	**See Also:**
Notes: May overwrite .BAK and .PAS files if not enough .COM files are available in a directory for it to infect. Infected files begin with "PQVWS". They also contain the string "combakpas???exe" at offset 0x17.0 VIRSCAN string..... BF00018B360C0103F7B95D021E07EA00, scan COM files only.		

Name: ANTI-PCB		
Aliases: ANTI-PCB	**Type:** Trojan.	
Disk Location: ANTI-PCB.COM	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Apparently one RBBS-PC sysop and one PC-BOARD sysop started feuding about which BBS system is better, and in the end the PC-BOARD sysop wrote a trojan and uploaded it to the rbbs SysOp under ANTI-PCB.COM. Of course the RBBS-PC SysOp ran it, and that led to quite a few accusations and a big mess in general.		

Name: AntiCAD		
Aliases: AntiCAD, Plastique-B, Plastique 2, Plastique 5.21, Plastique, Invader, HM2	**Type:** Boot sector.	
Disk Location: COM application.EXE application.COMMAND.COM. Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.Multipartite	
Damage: Corrupts a program or overlay files.Corrupts a data file.	**Size:** 2576290030043012 4096	**See Also:** Jerusalem, Jerusalem.AntiCAD. 4096
Notes: Story on first sighting May 1990 in virus-l, v5-059 plays tunes, infects both boot sectors and executable files. Derived from the Jerusalem virus. Targeted against the AutoCAD program. When ACAD.EXE is run the viruses will activate, overwriting data on floppy disks and hard disks, as well as garbling the contents of the CMOS.		

Name: AntiCMOS		
Aliases: AntiCMOS, AntiCMOS.B, Lenart, Anti CMOS	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR above TOM.Uses 2048 bytes above TOM	
Damage: Corrupts CMOS Configuration	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: CPAV calls it Lenart, F-Prot calls it AntiCMOS.B AntiCMOS is a primitive floppy disk boot sector and hard disk partition sector infector. It is buggy and causes unintentional hangs as well as its intended payload. If the virus triggers, it destroys the setup configuration in the CMOS memory. This may convince users that their hard disk has been wiped, but it is undamaged. The sytem just doesn't know it is there anymore. Restoring the setup information will bring it back. You shouldn't need an anti-virus to clean this if you have DOS 5 or 6. Just clean-boot the computer and use FDISK /MBR to replace the partition sector code on the hard disk. You also need to scan and clean all the floppy disks that have been in the machine(s). To clean floppies, copy the files off and reformat (with /u parameter to prevent unformatting), or use the SYS command (this won't work unless there is room for the DOS system files). F-Prot 2.19 can detect and remove it. Floppies that have had it removed are no longer bootable (if they were before infection) . The virus does not save the old floppy boot sector. It can remove the virus from the hard disk partition table without any problems. chkdsk shows 653,312 bytes of real memory without the virus there is 655,360 bytes. The virus hides at TOM and moves the TOM down by 2,048 bytes.		

Name: AntiEXE		
Aliases: AntiEXE, Anti EXE, AntiEXE.A, D3, NewBug, CMOS4.	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.Stealth; actively hides from detection.Identified by a one-kilobyte memory loss during booting.	
Damage: Corrupts hard disk partition tableCorrupts floppy disk boot sectorPossibly contains a destructive payloadCorrupts the image of certain EXE files	**Size:** Overlays boot sector, no increase	**See Also:** Genb

Notes: AntiEXE is detected by F-PROT2.10c.
Virhunt 4.0c and Scanv 106 call it a Generic Boot virus.
The virus hides in the boot sector of a floppy disk and moves the actual boot sector to cyl:0 side:1, sector: 15
On the hard disk, the virus infects the partition table, the actual partition table is on cyl: 0, Side: 0, sector: 13.
These are normally unused sectors, so disk data is not compromised by the virus insertion.
The virus uses stealth methods to intercept disk accesses for the partition table and replaces them with the actual partition table instead of the virus code. You must boot a system without the virus in memory to see the actual virus code.
We don't yet know if there is a destructive payload attached to the virus, but the name AntiEXE is somewhat ominous.
Frisk thinks that " it checks if a disk buffer being written to a disk starts with "MZ" (the EXE file marker, and then does something, but I have never disassembled the virus properly, so I'm not 100% sure..."
No destructiveness has been observed.

An update to the above information which extracted from VB :
The payload specifically targets EXE files, it searches for an EXE file that is 200,768 byte long and has 3895 relocation items. If these criteria are met then the image of EXE file header read will be corrupted. The corruption in this case means that the file could not be loaded and any attempt to copy the file leads to the corruption of the EXE file. This method of operation and search shows that this virus is designed to attack a specific application. It has been suggested that the target is a Russian Anti-Virus program, However that has not been confirmed, yet. If we assume that AntiEXE is designed to attack a Russian AntiVirus program, then the unusual way in handling Int 13h and F9h are explained.

All read calls have a 3 in 256 chance of activating the virus payload. These probability are based on the least significant word of the BIOS RAM data area maintained by the timer at 0000:046Ch.

Removal of the virus must be done under clean sysytem condition (Re-boot from clean system floppy disk). The command FDISK/MBR can be used for DOS 5.0 or later versions. Otherwise, use a sector editot retrive the original MBS from Trak0, Sector 13, Head 0 and put it back into its correct location at Track0, Sector1, head 0.
The SYS command will remove virus from floppy disck. Since, the original boot sector is still somewhere on the floppy disk, it will be better to re-format the disk.

Warning: When AntiEXE is active, it infects diskettes in both A and B drives. The virus performs some calculation to chose the new location for the original boot sector. The virus overwrites the original boot sector to that area, and this could lead to the loss of data, file corruption, etc.

Name: Antimon		
Aliases: Antimon, Pandaflu	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 1450	**See Also:**
Notes: This virus is targeted against protection programs, Flushot and some programs from Panda Software.		

Name: AntiPascal		
Aliases: AntiPascal	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 605529	**See Also:**
Notes: This virus is supposed to have been written to take revenge against the former employer of the virus author.		

Name: AntiPascal II		
Aliases: AntiPascal II, Anti-pascal II, Anti-Pascal 400, Anti-Pascal 440, Anti-Pascal 480, AP-400, AP-440, AP-480	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 400440480	**See Also:** Anti-Pascal
Notes: A group of three viruses similar to the Anti-Pascal viruses, probably by the same author.		

Name: Antitelifonica		
Aliases: Antitelifonica, A-VIR	**Type:** Boot sector.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Encrypted	
Damage: Corrupts boot sectorCorrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A multi-partite virus, may be stealth too		

Name: Antix Trojan		
Aliases: Antix Trojan	**Type:** Trojan.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-137: Just delete it, nobody in their right minds would ever want to use it.		

Name: AOLGOLD		
Aliases: AOLGOLD, aolgold.zip, aol gold	**Type:** Trojan.	
Disk Location: aolgold.zip	**Features:**	
Damage: Deletes or moves files.	**Size:** none	**See Also:**

Notes: AOL discovered an e-mail message with the AOLGOLD.ZIP file attached. The file purports to be a new front end for AOL, but is actually a trojan that deletes files on your c drive.

AOLGOLD Trojan
==========

The AOLGOLD Trojan program was recently discovered on America Online (AOL). Notice about the Trojan has been circulated to all America Online subscribers. Notice about the Trojan and a copy of the Trojan program were supplied to CIAC by Doug Bigelow in AOL operations.

Apparently, an e-mail message is being circulated that contains an attached archive file named AOLGOLD.ZIP. A description that accompanies the archive describes it as a new and improved interface for the AOL online service. Note that there is no such program as AOLGOLD. Also, simply reading an e-mail message or even downloading an included file will not do damage to your machine. You must run the downloaded file to release the Trojan and let it do damage.

If you unzip the archive, you get two files: INSTALL.EXE and README.TXT. The README.TXT file again describes AOLGOLD as a new and improved interface to the AOL online service. The INSTALL.EXE program is a self extracting ZIP archive. When you run the install program, it extracts 18 files onto your hard drive:

MACROS.DRV
VIDEO.DRV
INSTALL.BAT
ADRIVE.RPT
SUSPEND.DRV
ANNOY.COM
MACRO.COM
SP-NET.COM
SP-WIN.COM
MEMBRINF.COM
DEVICE.COM
TEXTMAP.COM
HOST.COM
REP.COM
EMS2EXT.SYS
EMS.COM
EMS.SYS
README.TXT

The file list includes another README.TXT file. If you examine the new README.TXT file, it starts out with "Ever wanted the Powers of a Guide" and continues with some crude language. The README.TXT file indicates that the included program is a guide program that can be used to kick other people off of AOL.

If you stop at this point and do nothing but examine the unzipped files with the TYPE command, your machine will not be damaged. The following three files contain the Trojan program:

MACROS.DRV
VIDEO.DRV
INSTALL.BAT

The rest of the files included in the archive appear to have been grabbed at random to simply fill up the archive and make it look official.

The Trojan program is started by running the INSTALL.BAT file. The INSTALL.BAT file is a simple batch file that renames the VIDEO.DRV file to VIRUS.BAT and then runs it. VIDEO.DRV is an amateurish DOS batch file that starts deleting the contents of several critical directories on your C: drive, including:

c:\
c:\dos
c:\windows
c:\windows\system
c:\qemm
c:\stacker
c:\norton

It also deletes the contents of several other directories, including those for several online services and games, such as:

c:\aol20
c:\prodigy
c:\aol25
c:\mmp169
c:\cserve
c:\doom
c:\wolf3d

When the batch file completes, it prints a crude message on the screen and attempts to run a program named DoomDay.EXE. Bugs in the batch file prevent the DOOMDAY.EXE program from running. Other bugs in the file cause it to delete itself if it is run from any drive but the C: drive. The programming style and bugs in the batch file indicates that the Trojan writer appears to have little programming experience.

Recovery:

WARNING Do not copy any files onto your hard disk before trying to recover your hard drive.

The files are deleted with the DOS del command, and can be recovered with the DOS undelete command. The files are still on your disk, only the directory entries have been removed. If you copy any new files onto your hard disk, they will likely be written over the deleted files, making it impossible to recover the deleted files.

If you have delete protection installed on your system, recovery will be relatively easy. If not, the DOS undelete command can be used, but you will have to supply the first letter of each file name as it is recovered. In many cases, you will probably want to restore the directories by reinstalling them from the original installation disks, but do that last. You must recover any unreplaceable, files first using undelete and then replace any others by copying or reinstalling them from the distribution disks.

To recover the system:

1. Boot the system with a clean, locked floppy containing the recovery program for the recovery files you have installed, or the DOS UNDELETE.EXE program if you do not have recovery files installed.

2. Type the VIRUS.BAT file to get a list of the directories the Trojan tried to delete. Ignore any directories don't exist on your machine.

3. Run the recovery program and recover your files. You may have to help it find the recovery files, such as MIRROR, which will be in the root directory. You may have to recover the MIRROR file first and then use it to recover the other files.

If you are using only the DOS undelete command, type:

```
undelete directory
```

where directory is the name of the directory to examine. To undelete the files in the dos directory, use:

```
undelete c:\dos
```

The undelete program will present you with a list of deleted files with the first letter replaced with a question mark. Without delete protection, you will have to supply this letter in order to undelete the file.

4. After you have restored as many files as you want or can using the UNDELETE command, replace any others by reinstalling them using the original installation disks.

DOOMDAY
=========
The DoomDay.exe program is actually hidden in the macros.drv file. when you run it, the Trojan maker program appears. The trojan maker program creates quick basic programs to damage a system. It includes the quickbasic compiler and pklite for compressing the trojans.The programs created by it all hang, as they appear to be missing their end statement.

Name: April 1. EXE		
Aliases: April 1. EXE, Suriv 2, Suriv 2.01	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1488	**See Also:**

Notes: Same as the April 1. COM virus, displays

APRIL 1ST HA HA HA YOU HAVE A VIRUS.

on April 1st. Those two viruses were later combined into one, called SURIV 3, which evolved into the Jerusalem virus.

Name: Arab		
Aliases: Arab	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 834	**See Also:**
Notes:		

Name: Aragon		
Aliases: Aragon	**Type:** Boot sector.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: v6-144: There was a false alarm of Aragon due to a person's built-in virus protection of their hard disk controller's additional ROM. They switched off the ROM via jumper and the virus false alarm went away.		

Name: ARC513.EXE		
Aliases: ARC513.EXE, ARC514.COM	**Type:** Trojan.	
Disk Location: ARC513.EXEARC514.COM	**Features:**	
Damage: Corrupts boot sectorCorrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: ARC513.EXE This hacked version of ARC appears normal, so beware! It will write over track 0 of your [hard] disk upon usage, destroying the disk. ARC514.COM This is totally similar to ARC version 5.13 in that it will overwrite track 0 (FAT Table) of your hard disk. Also, I have yet to see an .EXE version of this program.		

Name: ARC533		
Aliases: ARC533	**Type:** Trojan.	
Disk Location: COMMAND.COMARC533.EXE	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: ARC533.EXE This is a new Virus program designed to emulate Sea's ARC program. It infects the COMMAND.COM		

Name: Arcv.companion		
Aliases: Arcv.companion	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Armagedon		
Aliases: Armagedon, Armagedon the first, Armagedon the Greek	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1079	**See Also:**
Notes: If a Hayes modem is installed, the virus dials 081-141, which is the number of the "speaking clock" on the island of Crete. v6-151: At least one anti-virus program can detect and remove Armagedon.1079.D.		

Name: Arriba		
Aliases: Arriba	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1590	**See Also:**
Notes:		

Name: Ash		
Aliases: Ash, Ash-743	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 280743	**See Also:**
Notes:		

Name: Astra		
Aliases: Astra	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 976	**See Also:**
Notes: Contains the text "(C) AsTrA, 1991".		

Name: AT		
Aliases: AT	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 132-149	**See Also:**
Notes: A group of 4 viruses that only run on an IBM AT computer.		

Name: AT II		
Aliases: AT II	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 108-122	**See Also:**
Notes: Group of small viruses that only work on an IBM AT computer.		

Name: Atas		
Aliases: Atas	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 384400	**See Also:**
Notes:		

Name: Athens		
Aliases: Athens	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1463	**See Also:**
Notes: This virus contains the following text message: TROJECTOR II,(c) Armagedon Utilities, Athens 1992		

Name: Atomic		
Aliases: Atomic, Toxic	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 480	**See Also:**
Notes: v6-151:Atomic overwrites/destroys infected files. For the variants Toxic, 166, 350 and 831 :At least one anti-virus program can detect and remove these viruses.		

Name: Attention		
Aliases: Attention, Attention!, Attention.C	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: This virus gets its name from the string "ATTENTION" which is near the beginning of infected files. Originated in USSR. v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Aurea		
Aliases: Aurea	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Australian Parasite.272		
Aliases: Australian Parasite.272	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Auto		
Aliases: Auto	**Type:** Program.	
Disk Location: COM application.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 129	**See Also:**
Notes:		

Name:AZUSA		
Aliases: AZUSA, Azuza, Hong Kong, Sylvia	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk partition tables.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts a program or overlay files.Disables com1 and lpt1Corrupts a data file.Corrupts floppy disk boot sectorCorrupts hard disk partition table	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: AZUSA is a boot sector and partition table infector that is at least as effective as the STONED and infects the boot sectors of floppies and the partition table of hard disks. It goes resident and takes 1k of memory from the TOM (CHKDSK "total bytes memory" is reduced by 1024 bytes - 640k machine will report 654336 instead of 655360). No stealth is involved and it may be recognized by the long jump (E9 8B) at the start of an infected sector. It causes bombs by disabling COM1 and LPT1. Found on distribution disks of TVGA - 8916 (Trident Microsystems, Inc.) VGA software. System crashes. The computer is not able to talk to COM1 and LPT1., Top of memory reduced by 1K. long jump (E9 8B) at the start of an infected sector. For floppies, boot with an uninfected disk and use the sys command to rewrite the boot blocks. A hard disk must have its partition table restored from a copy stored on a floppy. Most of the tools programs do this (PC Tools, Norton, etc.) though you must save the copy before the disk is infected.		

Name: Backfont		
Aliases: Backfont	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 905765900	**See Also:**
Notes: Appears to change the font on VGA/EGA displays. Font changes on VGA or EGA displays.		

Name:BACKTALK		
Aliases: BACKTALK	**Type:** Trojan.	
Disk Location: BACKTALK.???	**Features:**	
Damage: Overwrites sectors on the Hard Disk.	**Size:**	**See Also:**
Notes: This program used to be a good PD utility, but someone changed it to be trojan. Now this program will write/destroy sectors on your [hard] disk drive. Use this with caution if you acquire it, because it's more than likely that you got a bad copy.		

Name: Bad Boy		
Aliases: Bad Boy	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 10001001	**See Also:**
Notes: The virus contains the following text: Make me better! The Bad Boy virus, Version 2.0, Copyright (C) 1991.		

Name: BadSector		
Aliases: BadSector, Bad Sector	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Baobab		
Aliases: Baobab	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1635	**See Also:**
Notes:		

Name: Barrotes		
Aliases: Barrotes	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes:		

Name: Bebe		
Aliases: Bebe, Bebe-486	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 1004486	**See Also:**

Notes: This virus contains the following pieces of text:

VIRUS! Skagi "bebe" Fig Tebe !

The variant, Bebe-486 is shorter and does not contain the text.

Name: Best Wishes		
Aliases: Best Wishes, Best Wishes-B, Best Wishes-970	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1024970	**See Also:**

Notes: The virus contains the following text:

This programm ... With Best Wishes!

COMMAND.COM, will not work properly when infected.

The variant Best Wishes-970 , or Best Wishes-B is shorter and damages .EXE files trying to infect them.
v6-151: At least one anti-virus program can detect and remove Best Wishes (1024.C and 1024.D).

Name: BetaBoys		
Aliases: BetaBoys, Mud	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 575	**See Also:**
Notes: Written by the same authors who wrote the Swedish Boys viruses.		

Name: Beware		
Aliases: Beware, Monday 1st	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Overwrites sectors on a Floppy disk.	**Size:** 442	**See Also:**
Notes: The virus contains the text BEWARE ME - 0.01, Copr (c) DarkGraveSoft - Moscow 1990 It activates Monday the 1st, overwriting the first sectors of any diskette in drive A: Trashed Floppy disks on a Monday the 1st.		

Name: BFD		
Aliases: BFD, Boot-EXE	**Type:** Boot sector.	
Disk Location: EXE application.Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 512	**See Also:**
Notes: The virus is very small, and infects .EXE files by inserting itself in the unused space between the file header and the actual start of the code. v6-151: At least one anti-virus program can detect and remove Bootexe.		

Name: Big Joke		
Aliases: Big Joke	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 1068	**See Also:**
Notes: The virus contains the text, At last ..... ALIVE !!!!! I guess your computer is infected by the Big Joke Virus. Release 4/4-91 Lucky you, this is the kind version. Be more careful while duplicating in the future. The Big Joke Virus, killer version, will strike harder. The Big Joke rules forever		

Name: BIO		
Aliases: BIO	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Mac and pc version, attacks only Microsoft products		

Name: Bit Addict		
Aliases: Bit Addict	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Erases the Hard Disk.	**Size:** 477	**See Also:** Crusher
Notes: This virus may trash hard disks, and then display the message: The Bit Addict says: "You have a good taste for hard disks, it was delicious !!!"		

Name: Black Jec		
Aliases: Black Jec, Sad, Digital F/X	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 231 to 440	**See Also:**
Notes: A family of at least 11 small viruses. The variant, Digital F/X crashes many machines. The variant, Sad activates in Sept, and contains the text Sad virus - 24/8/91 v6-151: At least one anti-virus program can detect and remove Black Jec (284, 323 and 235).		

Name: Black Monday		
Aliases: Black Monday, Borderline	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1055781 - Borderline veriant	**See Also:**
Notes: The virus contains the text, Black Monday 2/3/90 KV KL MAL The variant, Borderline can only infect .COM files. v6-151: At least one anti-virus program can detect and remove Black Monday (1055.E, 1055.F, 1055.G and 1055.H)		

Name: Blood		
Aliases: Blood, Blood 2	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 418	**See Also:**
Notes: Infected programs may occasionally display the following message when they are executed. File infected by BLOOD VIRUS version 1.20 The variant, Blood-2, probably does not exist.		

Name: Blood Rage		
Aliases: Blood Rage, BloodRage	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: BloodLust		
Aliases: BloodLust	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 302	**See Also:**
Notes: The virus contains the text, Hi! This is the virus BloodLust striking! Sorry to tell you, but your system is infected.		

Name: Bloody!		
Aliases: Bloody!, Beijing, June 4th	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: The Bloody! virus (aka Beijing or June 4th) is a boot sector virus. You cannot get it by downloading files - you must try to boot from an infected diskette.		

Name: Bloomington		
Aliases: Bloomington, NOINT, Stoned III, Stoned 3	**Type:** Boot sector.Direct acting. Activates when run.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Encrypted	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: "stealthy" MBR and boot sector infector. Not a very forgiving virus, if you look for the partition table you are likely to get garbage, and if DOS gets garbage, the disk is gone. CHKDSK will report 2k less "total bytes memory" (640k reporting 655360-653 or less is a danger sign) Named NoInt by Micke McCune when isolated in MAY 91 , it doesn't use interrupts to send commands to BIOS. McAfee calls it Stoned III for some random reason, Norton AntiVirus calls it Bloomington (town of its discovery)		

Name: Blue_Nine		
Aliases: Blue_Nine, Blue Nine	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.Stealth	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Bob		
Aliases: Bob	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 718	**See Also:**
Notes: This virus activates in January 1993.		

Name: Bob Ross		
Aliases: Bob Ross, Beta	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:** Screaming Fist virus
Notes: Rumor: written by the group PHALCON/SKISM (like Screaming Fist virus) Polymorphic because it changes one byte in the middle of the decryption routine		

Name: Bones		
Aliases: Bones, Stoned-T, NOP	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR above TOM.Stealth	
Damage: Trashes the hard disk.On the 7th of any month it reatrranges the data on the hard disk.	**Size:** Overlays boot sector, no increaseReduces RAM by 1K.	**See Also:**

Notes: The virus is detected as Bones, Stoned-T, or NOP by different anti-virus products.

********VirHUNT 4.0E does not detect it**********

VirALERT does detect and stop the attempted infection, but VirHUNT 4.0E can not detect or identify it.
F-PROT 2.16 calls it Bones
Norman calls it Bones
Vi-Spy 12 calls it Stoned-T
SCAN 2.14e calls it NOP

The virus uses stealth techniques, so most packages will not be able to detect it with the virus in memory. Most packages did discover the virus string in memory though they could not see the virus on disk.

The virus is very destructive. On the 7th of any month, it will rearrange the data on your hard drive the first time you access an uninfected floppy. You can not recover from the destruction. All data on the hard drive is lost.

Before it triggers, the virus can be removed by booting from a locked floppy and executing FDISK /MBR to write a new master boot record.

The virus loads at the top of memory and moves the top of memory down by 1K. Run MEM under DOS and you get back 654,336 bytes of memory instead of 65,360, a difference of 1K bytes.

The virus is tiny, fitting on a single sector on disk (<512 bytes).

Name: Boojum		
Aliases: Boojum	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 334	**See Also:**
Notes:		

Name: Boot 437		
Aliases: Boot 437, boot-437	**Type:** Boot sector.	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: v6-126: It's a rather unremarkable MBR infector of Polish origin. Infects the boot sector of diskettes and the MBR of hard disks. The original boot sector is moved to cylinder 0, side 0, sector 6 on hard disks and to the last sector of the root directory on floppies. It is not intentionally destructive and in fact has no payload at all. Can be removed with FDISK/MBR (from DOS 5.0 or higher) from the hard disk.		

Name: Boys		
Aliases: Boys	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 500	**See Also:**
Notes: When this virus finds no more .COM files to infect, it starts deleting .EXE files.		

Name: Brain		
Aliases: Brain, Pakistani, Ashar, Shoe, Shoe_Virus, Shoe_Virus_B, Ashar_B, UIUC, UIUC-B, @BRAIN, Jork, Shoe B	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorInterferes with a running application.Corrupts a data file.Corrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: This virus only infects the boot sectors of 360 KB floppy disks. It does no malicious damage, but bugs in the virus code can cause loss of data by scrambling data on diskette files or by scrambling the File Allocation Table. It does not tend to spread in a hard disk environment. Diskette volume labels changeto "(c) Brain".		

Name: Brasil Virus		
Aliases: Brasil Virus, Brazil	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.Encrypted	
Damage: Corrupts hard disk partition tableCorrupts floppy disk boot sectorOverwrites sectors on the Hard Disk.Overwrites part of the directory.	**Size:** Overlays boot sector, no increaseOverlays part of the directory	**See Also:**

Notes: The virus occupies three sectors of a disk. The first sector used is the boot sector in diskettes, or the master boot sector in hard disks.
The first sector contains the initial activation code.
The second sector contains the virus code that becomes memory resident, and that is responsible for propagating the virus.
In the third sector the virus stores the original boot sector.

In hard disks the virus uses sectors1, 2 and 3 of cylinder zero, head zero.
To eliminate this virus, sector 3 (the original master boot) should to be copied back into sector 1.

In 360k diskettes the virus uses DOS sectors 0, 10 and 11 (this means sector 1, cyl. 0, track 0 (boot), sec 2 cyl 0 tr. 1 (sector 10 and sect 3 cyl 0 tr. 1 (sector 11)). Sectors 10 and 11 are the end sectors of the root directory, and the virus may overwrite directory information during the infection process.
To eliminate the virus sector 11 into should be copied back into sector 0.

The virus handles correctly other diskette types (720k, 1.2M and1.44M), hiding his three sector always in the boot sector and in the last two directory sectors.

The virus triggers by decrementing a counter once for every hour of operation. After 120 hours of effective use, the virus writes his message ("Brasil virus!"), writes random data in the first 50 cylinders of the hard disk and the "freezes" the computer.

F-Prot 2.09D detects it. Scan 106 detects a non-standard boot sector. Virhunt 4.0B does not detect it.

Name: Breeder		
Aliases: Breeder, Shield	**Type:** Companion and Trojan program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 5152Adds File	**See Also:**

Notes: In addition to its operation as a regular "companion" type virus, this virus will append a 172 byte Trojan to COM files, which may display the message:

> I greet you user.
> I am COM-CHILD, son of The Breeder Virus.
> Look out for the RENAME-PROBLEM !

Name: Brunswick		
Aliases: Brunswick, 910129	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The Brunswick virus infects the boot sector/master boot record of hard disks and floppies in drives A: and B: only. Once resident, this virus covertly infects all floppies and hard disks it contacts. An infected machine does not display any obvious indications of infection; therefore it can be very difficult to determine if your system is infected until the attack phase commences. During the attack phase, it overwrites the boot sector with random characters. None until it starts destroying boot records, then formerly bootable disks become unbootable. VIRHUNT v. 1.3D-1, VIRSCAN v.2.0.2 and others VIRHUNT v. 1.3D-1, VIRSCAN v.2.0.2 and others. Boot from an uninfected Floppy and rewrite the boot with the DOS SYS command.		

Name: Bryansk		
Aliases: Bryansk	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 673	**See Also:**
Notes: The virus activates on Fridays, before 3PM When activated, it makes files read-only. The virus contains the text, BRYANSK 1992, BITE 0.01 (C)		

Name: Budo		
Aliases: Budo	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 890	**See Also:**
Notes: The virus contains the strings, "FLOW LIKE A RIVER - STRIKE LIKE A THUNDER" "Run time error" "Run time error" is displayed if an infected program is run when the virus is already resident.		

Name: Bulgarian 800		
Aliases: Bulgarian 800, 800	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 800	**See Also:**
Notes:		

Name: BUPT		
Aliases: BUPT, Traveler	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 12201223	**See Also:** Buptboot
Notes: Originated in the USA. The virus contains the following text, Traveller (C) BUPT 1991.4 Don't panic I'm harmless v6-151: At least one anti-virus program can detect and remove Bupt.1279		

Name: Buptboot		
Aliases: Buptboot, Welcomeb, Welcomb	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** Overlays boot sector, no increase	**See Also:** Bupt
Notes: Typical boot infector, but does not preserve a copy of the boot sector. The virus ontains the text: Welcome to BUPT 9146,Beijing!		

Name: Burger		
Aliases: Burger, 505, 509, 541, 909090H, CIA, Virdem 792, Virdem 2, Bustard, Cheater	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Not widespread at all v6-151: Overwrites/destroys infected files. At least one anti-virus program can detect and remove Virdem (1336.Bustard.A, 1336.Bustard.B and 1336.Cheater)		

Name: Burger		
Aliases: Burger, Burger 382, 382 Recovery, Burger 405, 405, Lima, Pirate, 560-A, 560-B, 560-C, 560-D, 560-E, 560-F, 560-G, 560-H	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 560382 - Burger 382, 382 Recovery405 - Burger 405609 - Pirate, Lima	**See Also:**
Notes: Overwrites .COM files At least eight 560 byte variants are known, named Burger 560-A, Burger 560-B etc. The variant, Burger 405 contains an error that allows it to reinfect files over and over.		

Name: Burghoffer		
Aliases: Burghoffer	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 525	**See Also:**
Notes:		

Name: Butterfly		
Aliases: Butterfly, Goddam Butterflies, Crusades	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:**	**See Also:** Civil War
Notes: Discovered in two files on the CIX online system in the UK, DOCUMENT.COM and SPORTS.COM The variant has the string "Hurray the crusades" in it. This virus is not a fast infector, and spreads slowly. It adds 302 bytes to COM files. There is no payload. The virus does not go memory resident. It avoids infecting COMMAND.COM. does not infect EXE files, a third variant does infect EXE files, but infected programs of 3rd variant never work		

Name: BUTTHEAD		
Aliases: BUTTHEAD, BUA-2263, Big Caibua, Vienna.Bua	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.Encrypted	
Damage: Deletes or moves files.Corrupts hard disk boot sector	**Size:** 2263-2296	**See Also:**

Notes: This is a relatively unsophisticated virus, of a kind that doesn't normally spread very well in the wild. However, this virus did spread rapidly via an infected 'SCREEN SAVER' , namely, 'COOLSAVER.COM.

It is a non-resident infector of *.COM files in the current directory and on the PATH (COMMAND.COM files is excluded).
If the date is May 5, 1995 or after, and the time is between 3pm and 7pm, it will display its distinctive phallic screen effect. Also at these times, it will check an internal counter, and if the value in the counter is high enough, it will execute various damage routines. These damage routines include the creation of directories named "Caibua", "FUCK YOU", "EAT SHIT" and "BITE ME!", the erasing of the first file in the current directory on the default drive, and damaging the data on the C: drive by overwriting the system boot record, FATs, and other system areas.

The following signature may be put into a file called ADDENDA.LST in
the IBMAV directory to enable IBMAV to detect this virus:

51BE01018B1481C2F7058BF2FC90E88908
%s the Bua-2263 %s
(COM. Mismatches=01.)

Text in file: "NGiK"

It was also discovered on the CRS Online BBS in Canada, in the file: BESTSSVR.ZIP

A virus scanner is available at CRS in file area 1: XCAIBUA.ZIP

The BESTSSVR.ZIP file when uncompressed yields the program COOLSAVR.COM.
The program claims to be a screensaver, but when run it creates the "Big Caibua!" virus which only infects files ending in ".COM".
The free program XCAIBUA.ZIP locates infected files and renames them so that they can be deleted.
Infected .COM files cannot be recovered.

More info. can be found in VB, June 1995 issue.

Name: C-544		
Aliases: C-544, Paniker, vienna family	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 544 bytes	**See Also:**

Notes: see below in summary section 1st occurance mid 1990 in Leningrad, USSR On Friday the 13th, message appears Virus family: ideologically - Vienna
Infection mechanism: Searching path and current directory, use standard int 21 file functions No Interrupts, no Special clues Detection: Use the message as a identification string, Prevention: Any active monitor Removal: Remove infected files, no fugs this time
Direct detection: Infected files contain the readable strings: '*.COM', 'PATH=' and 'That could be a crash, crash, crash !' Marked files in the seconds field in directory.

Name: Caco		
Aliases: Caco, Trident	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: contains the string "(C) 1992 John Tardy / Trident"		

Name: Cancer		
Aliases: Cancer	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 740 or multiples of this actual length is only 228 bytes	**See Also:**
Notes: Cancer infects all .COM files in the current directory whenever an infected program is run. It will repeatedly infect a file. It adds 740 bytes to the beginning of a file. A variant of amsrad. Increasing file lengths. An infected file will contain the string "IV" at offset 3 in the COM file.		

Name: Cansu		
Aliases: Cansu, V, V-sign, Sigalit	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts hard disk partition tableCorrupts floppy disk boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Brasil

Notes: Strange Video effects
Seen in Queensland Australia.

The virus has two parts, the boot sector and the virus body. The boot sector contains a short routine which loads the virus body into memory and transfers control to it. The virus body is located in:

Cylinder 0, Head 0, Sector 4 + 5	Harddisk
Track 0, Head 1, Sector 2 + 3	5.25" DD
Track 0, Head 1, Sector 13 + 14	5.25" HD
Track 0, Head 1, Sector 4 + 5	3.5" DD
Track 0, Head 1, Sector 14 + 15	3.5" HD

On floppy disks these sectors are the last two sectors of the root directory.

When executed, the virus goes memory resident and hooks interrupt vector 13 .

A bug causes floppy disks infected in drive B: to not work correctly. If you boot with such an
infected disk, the virus try's to load the virus body from drive B: instead of A:. If there isn't an infected disk in drive B, your system hangs.

There are two variants which differ in the payload trigger. After 64 (variant 1) or 32 (variant 2) infections in a system that has not been shut down or rebooted, it will display a "V" (Victory) sign on screen and hang the computer.

To remove the virus from a hard disk use the undocumented FDISK /MBR command which writes a new partition record without changing the partition table.

Detect with Virhunt 4.0B, SCANV106, fprot 209d, vispy 11.0.

Name: Capital		
Aliases: Capital	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 927	**See Also:**
Notes: Uses an encryption method similar to Cascade.		

Name: CARA		
Aliases: CARA	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1025	**See Also:**
Notes:		

Name: Carbuncle		
Aliases: Carbuncle	**Type:** Companion program.	
Disk Location: EXE application.Directory.	**Features:** StealthDirect acting. Triggering mechanism that corrupts 5 files each time.	
Damage: Renames files.When triggered, It overwrites the virus code in 5 files with *.CRP extension.	**Size:** Adds a File called carbuncle.com which is 622 bytes long. The *.EXE file renamed to *.CRP and creates a companion batch file *.BAT.	**See Also:**

Notes: 1. The virus spreads via an infected file, and as time go on the whole directory will be infected.
2. The infection routine creates a file called " CARBUNCLE.COM " which has the attributes of read _only and hidden.
3. The virus searches for any file with *.EXE. It renames the file to *.CRP and creates a companion batch file as *.BAT. When the user execute an infected file, the companion *.BAT is executed, since *.EXE files are no longer their . The *.BAT has the following lines:

```
@ECHO OFF
CARBUNCLE
RENAME  ....*.CRP .....*.EXE
.....*.EXE
RENAME ....*.EXE   ....*.CRP
CARBUNCLE
```

The method of infection and operation is quit clear from the above lines.The ECHO OFF command prevents the user from detecting any foul play in the system. The second line results in executing the various code and eventually more files are infected. The executable functions normally most of the time with a few error messages are issued.
4. The trigger routine is system time dependent. If the system time has a seconds field value less than 17, then the virus code is overwritten into 5 files with the extension of CRP. These files are damages and executing them will result in spreading the virus.
5. The virus is easy to detect and remove. Delete all BAT files and CARBUNCLE.COM file. Then, rename the CRP files to EXE . Some of the EXE files may contain the virus code which can be identified it contains the text string " PC CARBUNCLE:Crypt Newsletter 14 ".

Name: Carioca		
Aliases: Carioca	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 951	**See Also:** Faust
Notes: May be related to Faust		

Name: CARMEL TntVirus		
Aliases: CARMEL TntVirus	**Type:** Trojan.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This is a trojan suspect, Carmel Software Turbo Anti Virus package is a commercial package. If you did not purchase your copy or otherwise receive it directly from them, it could have a virus in it or otherwise be tampered. TAV has an "immunize" feature, if I recall correctly, that works by adding virus marker bytes (the signatures that viruses use to see if a file is infected) to the end of .COM and .EXE files. It could be that the files you immunized are self-checking and recognize that they have been modified.		

Name: Cascade		
Aliases: Cascade, 1704, 17Y4, 1704 B, 1704 C, Cascade A, Falling Tears, The Second Austrian Virus, Autumn, Blackjack, Falling Leaves, Cunning, Fall, Falling Letters, Herbst, Cascade YAP, YAP,Jo-Jo, Formiche	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedStealthDirect acting.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 17041701	**See Also:** 1701
Notes: Spreads between COM files. Occasionally causes odd screen behavior (the characters on the screen fall into a heap at the bottom of the screen!). One rare variant can destroy data on hard disks. see also 1701 Two different Cascade variants were called Cascade YAP. can be called YAP as well. Uses variable encryption, not polymorphic (virus-l, v5-097) The characters on the screen fall into a heap at the bottom of the screen! v6-151: At least one anti-virus program can detect and remove Cascade (691, 1701.G, 1701.H, 1701.J, 1701.K, 1701.L, 1704.L, 1704.N, 1704.O and 1704.P)		

Name: Casino		
Aliases: Casino, Malta	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts the file linkages or the FAT.	**Size:** 2330	**See Also:**
Notes: The virus offers to let you play a game, if you loose, It destroys the FAT on your hard disk. An offer to play an uninstalled game.		

Name: Casper		
Aliases: Casper	**Type:** Program.	
Disk Location:	**Features:** EncryptedDirect acting.Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: uses variable encryption		

Name: Catch 22		
Aliases: Catch 22, Catch-22	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: NOT A VIRUS! just a false report associated with Catch 2.2 loaded or resident. Was suspecious because it looked like it came from a Paint program.		

Name: CAZ		
Aliases: CAZ, CAZ-1159, Zaragosa	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 12041159	**See Also:**
Notes:		

Name: CC		
Aliases: CC	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 145	**See Also:**
Notes: Small virus that infects programs when they are executed.		

Name: CDIR		
Aliases: CDIR	**Type:** Trojan.	
Disk Location: CDIR.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This program is supposed to give you a color directory of files on your disk, but it in fact will scramble your disk's FAT table.		

Name: Chad		
Aliases: Chad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 751	**See Also:**
Notes: This virus contains the message, ... WOT!! No Anti - Virus		

Name: Chaos		
Aliases: Chaos	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorInterferes with a running application.Corrupts a program or overlay files.Corrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase	**See Also:** Brain
Notes: Derivative of Brain		

Name: Chaos		
Aliases: Chaos, Faust	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1181	**See Also:**
Notes: This virus contains the following encrypted text. CHAOS!!! Another Masterpiece of Faust... It appears to be related to the Carioca virus,		

Name: Checksum		
Aliases: Checksum, Checksum 1.01	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 123312321569 Variant infects COM and .EXE files	**See Also:**
Notes: A .COM file infector. The 1569 byte variant also infects .EXE files. v6-151: At least one anti-virus program can detect and remove Checksum.1253		

Name: Cheeba		
Aliases: Cheeba	**Type:** Program.	
Disk Location:	**Features:** EncryptedDirect acting.	
Damage:	**Size:**	**See Also:**
Notes: only virus that truely encrypts itself - uses a trivial kind of Vigenere cipher to encrypt its payload - V. Bontchev, v5-193		

Name: Chemnitz		
Aliases: Chemnitz	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 765	**See Also:**
Notes:		

Name: Chile Medeira		
Aliases: Chile Medeira, CPW, Mediera, Mierda?, 1530	**Type:** Program.	
Disk Location: EXE application.COM application.COMMAND.COM	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**
Notes: Two versions (at least) of a virus are pretty common in CHILE at the moment. These viruses infect COM's (including COMMAND.COM) and EXE's and erase files under some conditions. Both viruses are identified by SCAN106 and FPROT209. The original virus is reported as "CPW". The variant is reported as "Mediera" by Scan and "Mierda?" by FPROT. SCAN reports "1530" when the virus is active in memory. Do not panic. Just boot from a clean diskette and replace all infected COM's and EXE's with clean originals.		

Name: Chinese Fish		
Aliases: Chinese Fish, Chinese_Fish	**Type:** Boot sector.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-139: Chinese_Fish is not intentionally destructive. Any anti-virus program which can remove it, should leave your hard disk in its uninfected state. This virus stores the original MBR at cylinder 0, head 0, sector 10. Sector 9 of the first cluster on the hard disk says that "Fish will kill stone" or something like that. It displays its message on every disk access on the 1st, 11th, 21st, and 31st of every month in 1992, if the BIOS of the infected machine supports INT 1Ah (most ATs and above do).		

Name: Chris		
Aliases: Chris	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Christmas		
Aliases: Christmas, 1539, Father Christmas, Choinka, Tannenbaum, Christmas Tree, XA1, V1539	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Interferes with a running application.Corrupts boot sector	**Size:** 1539	**See Also:** Vienna
Notes: The virus infects .COM files when an infected application is executed. When an infected program is run between December 24th and 31st (any year), the virus displays a full screen image of a christmas tree and German seasons greetings. When an infected program is run on April 1st (any year), it drops a code into the boot- sectors of floppy A: and B: as well as into the partition table of the hard disk. The old partition sectors are saved but most likely destroyed since running another infected file will save the modified partition table to the same location. On any boot attempt from an infected hard disk or floppy, the text "April April" will be displayed and the PC will hang. "April April" printed at boot time then the machine hangs. A Christmas tree and German seasons greetings printed between 12/24 and 12/31. The virus contains the following German string: "Und er lebt doch noch : Der Tannenbaum !",0Dh, 0Ah,00h, "Frohe Weihnachten ...",0Dh,0Ah,07h, 00h (translated in English: "And he lives: the Christmas tree", "Happy Christmas")		

Name: Cinderella		
Aliases: Cinderella, Cinderella II	**Type:** Program.	
Disk Location: COM application.infects files of .DOC and .CO extension + more	**Features:** Memory resident; TSR.	
Damage: None found	**Size:** 390 bytes (Cinderella)779 bytes (Cinderella II)	**See Also:**
Notes: Found in Finland on Sept. 1, 1991, seems to be common in Finland but not much of anywhere else Bug in virus: Can infect non executible files, but these files won't spread the virus. Can't survive a warmboot. Not sure if it has a payload at all, infects every file opened or executed. Virus is only 390 bytes long Will infect files opened with a *.CO? pattern. tester had trouble trying to infect .DOC files though (v5-044) The virus counts keystrokes, and after some number creates a hidden file named CINDEREL.LA and then resets the computer. Reports exist for the virus creating a file CINDEREL.LA after a certain number of keys have been pressed.		

Name: Civilwar		
Aliases: Civilwar, Civil War, Trident, Dark Helmet, Civil War III	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 444	**See Also:**
Notes: contains internal string "Trident/Dark Helmet" v6-151: Civil War.444 overwrites/destroys infected files, but at least one anti-virus program can detect and remove Civil War III		

Name: Clone		
Aliases: Clone	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Brain
Notes: Derivative of Brain		

Name: Clonewar		
Aliases: Clonewar	**Type:** Companion program. Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 247	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Clonewar (238, 546, 923.A and 923.B)		

Name: Close		
Aliases: Close	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 656	**See Also:**
Notes: Attacks the system files IBMBIO.COM and IO.SYS. The system becomes unbootable.		

Name: Cls		
Aliases: Cls	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 853	**See Also:**
Notes: Occasionally clears the screen.		

Name: Cod		
Aliases: Cod	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 572	**See Also:**
Notes:		

Name: Code Zero		
Aliases: Code Zero	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Similar to VCL viruses.		

Name: Coib		
Aliases: Coib	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: College		
Aliases: College	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A virus that may have been developed at Algonquin college		

Name: Com2con		
Aliases: Com2con, USSR-311	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 311	**See Also:**
Notes: Origin is USSR		

Name: Comasp-472		
Aliases: Comasp-472	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 472	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Comasp.633		

Name: Commander Bomber		
Aliases: Commander Bomber, DAME	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.Polymorphic	
Damage:	**Size:**	**See Also:**

Notes: Written by "Dark Avenger" this virus infects by putting parts of itself in between commands of the executible file. Basically, the virus code is split up and exists in various places within the infected file.
Not encrypted, but you have to check the entire file for the virus.
attacks against known virus scanning techniques
v6-130: Try to find VirusBulletin December'92, page 10.
A brief info: It's a harmless memory resident polymorphic virus. It hooks int 21h and infects COM-file except COMMAND.COM on their execution. It contains the internal text messages "COMMANDER BOMBER WAS HERE" and "[DAME]". The characteristic feature of this infector consist of new polymorphic algorithm. Upon infection the virus reads 4096 bytes from the random selected offset and writes this code at the and of the file. Then it writes its code into this 'hole' and starts to polymorphism. This virus contains several subroutines which generate random (but successfully executed!) code, the virus inserts those parts of random code into the random chosen position into the host file. There are about 90% of all the i8086 instructions are present into those parts. The part of code takes the control from the previous part by JMP, CALL, RET, RET xxxx instructions. The first part is inserted into the file beginning and jumps to next part, the next part jumps the third etc. The last part returns control to the main virus body. At the end the infected file looks like at 'spots' of inserted code.

Name: Como		
Aliases: Como	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 2019	**See Also:**

Notes: The virus contains the following text message:

I'm a non-destructive virus developed to study the worldwide diffusion rate. I was released in September 1990 by a software group resident nearComo lake (north Italy).

Don't worry about your data on disk. My activity is limited only to auto-transferring into other program files. Perhaps you've got many files infected. It's your task to find and delete them
Best wishes

Name: Compiler.1		
Aliases: Compiler.1	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** 512

Notes: SCAN 97 says that Compiler.1 is the 512 virus (erroneously)

Name: Cookie		
Aliases: Cookie, Animus	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 73607392	**See Also:**

Notes: A large virus written in C or Pascal.

Name: Copyright		
Aliases: Copyright, 1193	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1193-1207 to COM files	**See Also:**

Notes: McAfee's program identifies it as Copyright [1193]
Has been distributed with a clone systems manufacturer along with some PD/shareware stuf & Jerusalem virus. Reported to infect .COM files incl COMMAND.COM, and load itself into RAM and remain resident, and directly or indirectly corrupt file linkages.
The virus contains the following fake copyright messages:

(C)1987 American Megatrends Inc.286-BIOS
(C)1989 American Megatrends Inc
(c) COPYRIGHT 1984,1987 Award Software Inc.ALL RIGHTS RESERVED
Infected executable will not run (giving a 'cannot execute' error or something similar) the first time an attempt is made, then will be either at that time or next time attempt is made, will delete it. CLEAN 86-B does not remove this virus

Name: Cossiga		
Aliases: Cossiga, Friends	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 8831361 - Friends variant	**See Also:** Arcv

Notes: The variant Friends contains the following text.

FRIENDS OF MAIS and CLAUDIA SAHIFFER

Name: CPL35.COM		
Aliases: CPL35.COM	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 478 bytes	**See Also:**

Notes: The virus appends to the end of host files. I t is not stealth

Name: Cpw		
Aliases: Cpw	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1459	**See Also:**

Notes: It contains the text

Este programa fue hecho en Chile en 1992 por CPW.

Name: Cracky		
Aliases: Cracky	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 546	**See Also:**

Notes: The virus contains the string,
"Cracky !"

Name: Crazy Eddie		
Aliases: Crazy Eddie	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.	
Damage: Erases the Hard Disk.	**Size:** Variable	**See Also:**
Notes:		

Name: Crazy Imp		
Aliases: Crazy Imp, Imp, Crazy	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 1445	**See Also:**
Notes:		

Name: Crazy_Nine		
Aliases: Crazy_Nine	**Type:** Program.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Stealth	
Damage: Does no damage.Infected machines crashes frequently	**Size:** a 4 kbytes long	**See Also:**
Notes: The following notes are extracted from VB, August 1995: Crazy_Nine is a 4 kbytes long, boot sector virus. This virus is build around the the low-level and the undocumented DOS and PC techniques. It takes advantage of these technique in eluding detection. The virus is an unusual kind; It is a polymorphic MBS type.		

Name: Creeper		
Aliases: Creeper, Creeping Tormentor, Creeper-425	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 475425	**See Also:**
Notes:		

Name: Crew-2048		
Aliases: Crew-2048	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 2048	**See Also:**
Notes: When infected programs are run, the 'European Cracking Crew' logo is sometimes displayed. The graphics screen contains the following text, This program is cracked by Notice this: TS ain't smart at all. Distribution since 11-06-1987 (or 06-11-1987) Press any key The variants have different messages.		

Name: Criminal		
Aliases: Criminal	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 2615	**See Also:** Ultimate Weapon
Notes: This virus contains the following text, Criminal, be a wiseguy and turn youreself in, if you don't I will The Ultimate Weapon has arrived, please contact the nearest police station to tell about the illegal copying of you This seems to be the same virus as the Ultimate Weapon listing, but the type is different.		

Name: Crooked		
Aliases: Crooked, Krivmous, Only	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 979	**See Also:**
Notes: This virus contains the text, Only God knows!		

Name: Cruncher		
Aliases: Cruncher, Trident, Cruncher 1.0, Cruncher 2.0, Cruncher 2.1	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Coffeeshop
Notes: contains internal string "[MK / Trident]" variation of Coffeeshop virus v6-126: 3 versions: 1.0, 2.0, 2.1. 2.1 asks permission all the time, The version number can be seen in plaintext in the infected files (along with other text and greetings to Dr. Cohen and the author of Diet), if you decompress them with Diet or UNP. Will infect a file without asking if you set the environment variable CRUNCH to AUTO.		

Name: Crusher		
Aliases: Crusher, Trident, Bit Addict	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: contains the internal string "Bit Addict / Trident"		

Name: CryptLab		
Aliases: CryptLab	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.Polymorphic	
Damage: Unknown, not analyzed yet.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Uses the MtE mutation engine.		

Name: CSL		
Aliases: CSL, Microelephant, CSL-V4, CSL-V5	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 381517457	**See Also:**
Notes: This virus contains the text, 26.07.91.Pre-released Microelephant by CSL		

Name: Cybercide		
Aliases: Cybercide	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: CyberTech		
Aliases: CyberTech	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: mentioned as rumor in May/June 1993 Infosecurity News, page 8 CIAC has article in full, believed that it displays the following message after Dec 31, 1992: "The previous year you have been infected by a virus without knowing or removing it. To be gentle to you I decide to remove myself from your system. I suggest you better buy ViruScan of McAfee to ensure to yourself complete security of your precious data. Next time you could be infected with a malevolent virus. May I say good-bye to your now...." [sic] after displaying the message, the virus supposedly disinfects the system, but that behavior has not been verified. v6-151: At least one anti-virus program can detect and remove Cybertech (501 and 503).		

Name: D-XREF60.COM		
Aliases: D-XREF60.COM	**Type:** Trojan.	
Disk Location: D-XREF60.COM	**Features:**	
Damage: Corrupts boot sectorCorrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: A Pascal Utility used for Cross-Referencing, written by the infamous `Dorn Stickel. It eats the FAT and BOOT sector after a time period has been met and if the Hard Drive is more than half full.		

Name: Da'Boys		
Aliases: Da'Boys, Da Boys, DaBoys, Dallas Cowboys	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** Overlays boot sector, no increase	**See Also:** Gold_Bug
Notes: Well written, difficult to detect virus. 8088 and 8086 based machines fail to boot from infected disks. Disables COM4. Sporadic reboots by infected machines. It loads itself into a hole in lower memory, it does not reduce the available memory indicated with chkdsk. It is a companion virus to the Gold_Bug virus. The Gold_Bug virus hides Da'Boys from the Windows 3.1 startup routines by removing it from the INT13 call chain when Wndows starts and reinstalling it after startup is complete.		

Name: Dada		
Aliases: Dada, da,da, yes,yes	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1356	**See Also:**
Notes: Contains the text, da,da (yes,yes in Russian).		

Name: DANCERS		
Aliases: DANCERS, DANCERS.BAS	**Type:** Trojan.	
Disk Location: DANCERS.BAS	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This trojan shows some animated dancers in color, and then proceeds to wipe out your [hard] disk's FAT table. There is another perfectly good copy of DANCERS.BAS on BBSs around the country.		

Name: Dark Apocalypse		
Aliases: Dark Apocalypse	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Dark Avenger		
Aliases: Dark Avenger, Dark Avenger-B, Black Avenger, Diana, Eddie, Rapid Avenger, Apocalypse-2, CB-1530, Milana, MIR, Outland, Ps!ko, Zeleng, Rabid, Jericho, Uriel, Dark_Avenger.1800.A	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Overwrites sectors on the Hard Disk.	**Size:** 1800	**See Also:** Zero Bug

Notes: Infects every executable file that is opened, .COM and EXE files are corrupted on any read attempt even when VIEWING!!! Every 16th infection, it overwrites a block of the hard disk with a copy of the boot block.
The virus construction kit may have used the Dark Avenger as a basis. This virus may have been based upon the Zero Bug virus.
Copies of the virus source code appear to have been passed out to others, resulting in the different variants.
The Rabid virus swapped 2 instructions, located in the center of a search string used by a well known scanner. Damaged files with "Eddie lives...somewhere in time" in them. "Eddie lives...somewhere in time" at beginning and
"This Program was written in the City of Sofia (C) 1988-89 Dark Avenger" near end of file

v6-147: (quote)
Do you know how a Dark_Avenger.1800.A infection looks like? Every program that the user has executed or opened (read or copied) is infected. Additionally, if the payload has activated, the virus has botched the hard disk here and there with sectors that contain the first 512 bytes of its body. Those sectors could be in a file, or in a subdirectory, or in the free disk space. Do you imagine how much time it will take to find all of them and determine to which files they belong on a reasonably large hard disk? On the other side, it will permit to find not only the infected files, but also the corrupted ones - but this is valid only for this particular virus.
And do you know what will happen after the user runs a disinfector? The virus will be truncated, the file beginning will be restored, but the virus body will most probably remain in the freed disk space. The next time the user runs your sector scanner, it will take exactly as much time as on an infected system - because it will continue to find the scan string here and there and will have to waste its time to compute that those sectors don't actually belong to files.

v6-151: At least one anti-virus program can detect and remove Dark Avenger (1800.F, 1800.G, 1800.H, 1800.I, 1800.Rabid.B, 2000.Copy.C, 2000.DieYoung.B, 2100.DI.B, Jericho and Uriel)

Name: Dark Avenger 3		
Aliases: Dark Avenger 3, Dark Avenger II, V2000, Die Young, Travel, V2000-B, Eddie 3, v1024, Dark Avenger III	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Corrupts a data file.Interferes with a running application.	**Size:** 2000	**See Also:**
Notes: Every 16 executions of an infected file, the virus will overwrite a new random data sector on disk; the last overwritten sector is stored in boot sector. The system hangs-up, if a program is loaded that contains the string "(c) 1989 by Vesselin Bontchev"; V.Bonchev is a Bulgarian author of anti-virus programs. Hex dump strings in code, Two Strings : 1) "Copy me - I want to travel" (at beginning of virus-code) 2) "(c) 1989 by Vesselin Bontchev" (near end of virus code; but V.Bontchev is not the author!)		

Name: Dark End		
Aliases: Dark End	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1188	**See Also:**
Notes:		

Name: Darth Vader		
Aliases: Darth Vader	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** 512
Notes: SCAN 97 says that Darth Vader virus is 512 virus (erroneously)		

Name: Dash-em		
Aliases: Dash-em	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1876	**See Also:**
Notes:		

Name: Dashel		
Aliases: Dashel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Datacrime		
Aliases: Datacrime, 1280, Columbus Day, DATACRIME Ib, Crime	**Type:** Program.Direct acting. Activates when run.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.Corrupts the file linkages or the FAT.	**Size:** 1280	**See Also:**
Notes: Spreads between COM files. After October 12th, it displays the message "DATACRIME VIRUS RELEASE: 1 MARCH 1989", and then the first hard disk will be formatted (track 0, all heads). When formatting is finished the speaker will beep (end-less loop). v6-151: At least one anti-virus program can detect and remove DataCrime (1168.B and 1280.B)		

Name: Datacrime II		
Aliases: Datacrime II, 1514, Columbus Day	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.Corrupts the file linkages or the FAT.	**Size:** 1514	**See Also:** 1168,1280
Notes: Spreads between both COM and EXE files. After October 12th, displays the message "* DATACRIME II VIRUS *", and damages the data on hard disks by attempting to reformat them.		

Name: Datacrime II-B		
Aliases: Datacrime II-B, 1917, Columbus Day, Crime-2B	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.	**Size:** 1917	**See Also:**
Notes: Spreads between both COM and EXE files. After October 12th, displays the message "* DATACRIME II VIRUS *", and damages the data on hard disks by attempting to reformat them.		

Name: Datacrime-B		
Aliases: Datacrime-B, 1168, Columbus Day, Datacrime Ia	**Type:** Program.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.Corrupts the file linkages or the FAT.	**Size:** 1168	**See Also:** Datacrime II
Notes: Spreads between COM files. After October 12th, it displays the message "DATACRIME VIRUS RELEASE: 1 MARCH 1989", and then the first hard disk will be formatted (track 0, all heads). When formatting is finished the speaker will beep (end-less loop).		

Name: Datalock		
Aliases: Datalock, Datalock 1.00, V920, Datalock 2, Datalock-1043	**Type:** Program.	
Disk Location: COM application.EXE application.Only .COM files > 22999 bytes long	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 9201043 - Datalock-1043 variant	**See Also:**
Notes: It infects all EXE files but COM files must be greater than 22999 bytes long. If a file is opened that matches the selector *.?BF (.DBF files) is will give the message "Too many files open" and prevent access to the file. From a report in virus-l, v4-220: system lock-ups, drop out of application with no messages. Some programs would display the message "overlay not found" prior to dropping to DOS, a .EXE file grew by 920 bytes during first execution and after re-installation. Using debugger, found string "DataLock version 1.0". Datalock 2 variant found in wild in DC area that is buggy(virus-l, v5-092) DATALOCK 2 does NOT contain string "Datalock version 1.0" SCAN 89b and FPROT 2.03a don't find Datalock 2 variant in EXE files, but original datalock signatures are valid and can be used to identify this variant. For DATALOCK 2: C3 1E A1 2C 00 50 8C D8 48 8E D8 81 2E 03 00 80 00 40 8E D8 v6-151: At least one anti-virus program can detect and remove DataLock (920.K1150 and 1740)		

Name: Day10		
Aliases: Day10, SYP	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Erases the Hard Disk.	**Size:** 674	**See Also:**
Notes: If the current date is divisible by 10, the virus trashes the hard disk.		

Name: Dbase		
Aliases: Dbase, DBF virus	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a data file.Interferes with a running application.Corrupts a program or overlay files.Corrupts the file linkages or the FAT.	**Size:** 1864	**See Also:**
Notes: Infects COM files. Registers all new .DBF files in a hidden file c:\BUGS.DAT. When any of those files are written, it reverses the order of adjacent bytes. When any of those files are read, it again reverses the bytes, making the file appear to be OK, unless it is read on an uninfected system or the file name is changed. When a file that is more than 3 months old is accessed, the virus attempts to destroy the FAT and root directory on drives D:, E;, ...Z:. Typical text in Virus body (readable with HexDump-utilities): "c:\bugs.dat" v6-151: At least one anti-virus program can detect and remove Dbase.E.		

Name: Dedicated		
Aliases: Dedicated, Fear	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.Polymorphic	
Damage: No damage, only replicates.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Uses the MtE mutation engine to hide.		

Name: Deicide		
Aliases: Deicide, Decide, Deicide II	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** Overlays application, no increase1335 (Deicide II variant)	**See Also:**
Notes: When activated, the virus destroys the first 80 sectors on drive C: The virus contains the following text: DEICIDE! Glenn (666) says : BYE BYE HARDDISK!! Next time be carufull with illegal stuff. This experimental virus was written by Glenn Benton to see if I can make a virus while learning machinecode for 2,5 months. (C) 10-23-1990 by Glenn. I keep on going making virusses.		

Name: Dejmi		
Aliases: Dejmi	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Demolition		
Aliases: Demolition	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 1585	**See Also:**
Notes:		

Name: Demon		
Aliases: Demon	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase	**See Also:**
Notes:		

Name: DenZuk		
Aliases: DenZuk, Venezuelan, Search, DenZuc B, Den Zuk, Mardi Bros, Sudah ada vaksin, Denzuko, Ohio, Hacker	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR above TOM.	
Damage: Interferes with a running application.Corrupts boot sector	**Size:** Overlays boot sector, no increaseUses1 boot sector and 9 sectors on track 40	**See Also:**
Notes: Infects floppy disk boot sectors, and displays a purple DEN ZUK graphic on a CGA, EGA or VGA screen when Ctrl-Alt-Del is pressed. F-Prot calls it Mardi Bros (virus-l, v5-072), but viruSafe says it is a different virus Discovered July 1990 in France, this virus installs itself 7168 bytes above high memory. Infected diskettes have their volume lable changed to "Mardi Bros" Boot sector will contain the following message "Sudah ada vaksin" The label on an infected disk will read: "Y.C.1.E.R.P", where the "." is the F9h character. from virus-l, v6-107: Denzuko is probably the first PC virus to format and store data on an extra diskette track. This elegantly avoids the corruption of directory and file information that most other boot sector viruses are likely to cause, and the sudden appearance of "BAD clusters" that Brain causes. However not all disk drives can access the extra tracks, and the disk media becomes less reliable near the centre of the disk.		

Name: Destructor		
Aliases: Destructor	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1150	**See Also:**
Notes: The virus contains the text, DESTRUCTOR V4.00 (c) 1990 by ATA v6-151: At least one anti-virus program can detect and remove Destructor.B.		

Name: Devil's Dance		
Aliases: Devil's Dance, Mexican, 941, 951	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Corrupts a data file.Corrupts the file linkages or the FAT.Overwrites sectors on the Hard Disk.	**Size:** 941, 951?	**See Also:**

Notes: Infects all .COM files in the current directory multiple times. Pressing Ctrl-Alt-Del displays

DID YOU EVER DANCE WITH THE DEVIL IN THE WEAK MOONLIGHT ?
PRAY FOR YOUR DISKS!!
The Joker

The virus counts keystrokes. After 2000 it activates, and and changes the screen colors, after 5000 it destroys the FAT
The file date/time is set to the date/time of the infection (i.e. multiple infected files have the same file date/time).
All characters typed will be displayed in a different color on a color card.
If <CTRL>+<ALT>+<DEL> is pressed, the following message is displayed:
"Have you ever danced with", "the devil under the weak light of the moon? ", "Pray for your disk! The_Joker...", "Ha Ha Ha Ha Ha Ha Ha Ha Ha Ha". Typical text in Virus body, readable with hexdump-utilities: "Drk", "*.com". If the high- bit of the displayed code is stripped, the message displayed at system reset time can be read. .COM files: the first three bytes (jmp) and the last three bytes are identical. The file date/time is set to the date/time of the infection (i.e. multiple infected files have the same file date/time).
v6-151: At least one anti-virus program can detect and remove Devil's Dance (C and D).

Name: Dewdz		
Aliases: Dewdz	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 601	**See Also:**

Notes: When this virus activates it displays the text

Kewl Dewdz!

The virus contains the string,

Made in STL (c) '91

Name: Diamond		
Aliases: Diamond, Italian Diamond, Damage, Damage-2, David, Greemlin, Lucifer, Rock Steady, Alfa, 1024	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk.Only the Rock Steady variant does this.	**Size:** 1024666 - Rock Steady Variant	**See Also:**

Notes: mentioned in Virus-l, v4-224, v5-006
Two variants were once uploaded to a BBS in Bulgaria.
Relative of 1024/1024B
The Rock Steady variant formats the hard disk on the 13th of any month.

Name: Dichotomy		
Aliases: Dichotomy, Evil Avatar	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Memory resident; TSR.PolymorphicInfection method of hard disk is different from flop disk	
Damage: Causes system to hang.Corrupts some EXE file.	**Size:** Polymorphic: each infection different2 block, 296 byte and 567 byte.	**See Also:**

Notes:
The following notes are extracted from VB:

The name is taken from an internal text string ' [Dichotomy] (c) 1994 Evil Avatar [Dichotomy] ' in the program.
The virus consists of two block, the loader block (296 byte) and the installation block (567 byte). On hard disk, the two block are copied in to two different files. On floppy disk, both blocks are copied into the same file, thus insuring the spread of the infection.
On hard disk, the virus appends the loader section to the end of the host file and replaces the first 3 bytes with jump instruction to the appended virus code. The installation block will be appended to the end of a second host file with no changed to the header and the body of this host file. The installation block functions are to install the virus in memory and to intercept the Int 21h handler.
On floppy disk, the virus infects host file with both sections, thus an infected file contains the whole virus code.

When a file infected with the loader code is run, the control is passed to virus code. The virus code searches for a predetermined file contains the installation block. When the file is located, the reminder of the virus code is loaded to memory. Now, virus checks the installation code for an identification word, 445Bh. If the ID is positive, then the virus checks to see whether there is a copy resident in memory. If there is a resident copy in the memory ,then control is returned to the host file. Otherwise it installs itself in memory. The process consists of allocating block of system memory, copying the virus code into it, modifying an undocumented Memory Control Block area, and hooking the Int 21h. Finally, it restores the host program header and returns control to the host program.

After infection, the virus modifies the date and time stamps of the host file.For host files infected by the loader section, the seconds value is set to 60. For files containing the installation block, the seconds value is set to 62. On floppy disk, the seconds value is set to 62,only. The virus used this stamp to distinguish between infected and clean files only.

Dichotomy has several bugs or missing instructions in the code. The most important one is that it infects EXE files as if they were COM files. When an infected EXE file is executed, its misidentified as a COM file, which causes the system to hang! The second important bug is related correct way of checking error flags and file length, and this will result in corrupting very short executable files.

The suggested method for disinfection is to use clean system for booting. Then identifiy the infected file and remove them. The Hex pattern canbe used to scan system memory. The pattern are:

```
Part1 : E800  008B  DC8b  2F81  ED03  0044
        443E  81BE  5203  5B44  B41A  8D96
Part2 : FEC4  80FC  4C74  32FE  CC80  FC51
        740C  80FC  6274  052E  FF2E  8C03
```

Name: Die Hard		
Aliases: Die Hard, DH2, Die_Hard. Diehard	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** EncryptedStealthMemory resident; TSR.	
Damage: Overwrites ASM and PAS files.Display messages	**Size:** EXE and COM files grow by exactly 4000 bytes	**See Also:**

Notes: NOTE: This information is second-hand, and still preliminary]
(from VIRUS-L newsletter v07i092.txt): Die_Hard is a resident fast infector of COM and EXE files. It is known to be in the wild in at least India, where it was found in September 1994.

The virus stays resident in memory, decreasing the available DOS memory by 9232 bytes. Die Hard infects all executed or opened COM and EXE files. The files grow by exactly 4000 bytes.

Die Hard has several layers of encryption. Once encrypted, the following text is found: SW DIE HARD 2
The encryption is not polymorphic, so the virus is quite easy to find. The virus maintains a generation counter, but it is currently not known if this information is used, or whether the virus has any activation routine at all.

F-PROT 2.18e and up will detect and remove the virus.
SCAN v. 224e will detect and remove it.
Thunderbyte Antivirus v. 635 will detect and remove it.
TBAV 6.26 and Normon Data Defense will detect it.
VirHunt 4.0E does not detect it.

Antiviral Toolkit Pro ver 2.1b by Eugene Kaparsky seems to clean it -- another method is:

1) Load the virus in the memory
2) Copy all infected files to another extension (e.g. .EXE to .999 and .COM to .998) and the virus will remove itself from the file
3) Warm boot the system with a clean bootstrap
4) Delete all infected files
5) Replace the COMMAND.COM file
6) Rename all files back to the correct extensions (see the earlier step)
[Thi s note from a 1994 issue of VIRUS-L by Gerald Khoo]

Update info. from VB, August 1995:
The virus intercepts Int 21h, Int 10h, Int 08h, Int 13h, Int 24h, and Int 40h. The method used to hooking interrupts are unusual, the virus inserts itself into the chain of programs hooking interrupts.
The virus hooks Int 21h on permanent bases.
It has several trigger routines. On any Tuesday, which is the 3rd, 11th, 15th, and 28th day of the month, the virus calls the DOS function Write, and displays the following message:
SW Error
The second trigger routine writes strings into PAS and ASM source files. When infected PAS or ASM files are compiled, the compiled programs displays Chinese character on the screen which are from bytes D1h and A5h.
The third trigger routine is executed after the virus generation is 15 and the current video mode is 13h. The screen displays 'SW" in large violet symbols.

.

Name: Digger		
Aliases: Digger	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1475 COM1478 EXE	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Digger.600		

Name: Dima		
Aliases: Dima	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1024	**See Also:**
Notes:		

Name: DIR		
Aliases: DIR	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Does no damage, doesn't affect any part of machine	**Size:** 691	**See Also:**
Notes: Only infects files when the DIR command is executed.		

Name: Dir II		
Aliases: Dir II, Dir 2, MG series II, Creeping Death, DRIVER-1024, Cluster, D2, Dir2	**Type:** Program.Memory resident.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Encrypts the file directory.Corrupts the file linkages or the FAT.Overwrites sectors on the Hard Disk.	**Size:** Adds File 1024places virus code in last cluster of infected disk and changes directory structure to have the cluster pointer of an executible file point to the viral executible.	**See Also:**

Notes: Cannot infect NetWare volumes, MS-Windows crashes upon infection
This virus modifies entries in the directory structure, causing the computer to jump to the virus code before execution of the program begins. This virus also uses stealth techniques to hide its existance in memory.
Initial infection occurs when a file with an infected directory is executed. The virus becomes memory resident by appearing to be a disk device driver, and puts a copy of itself on the last cluster defined as "good" in the disk. It then infects all .EXE and .COM file directory entries by scrambling the original cluster pointer, placing it in an unused section of the directory structure, and replacing the cluster with a pointer to the virus.
There are 5 variants (11/20/91). NOTE: This works on MS DOS ver 3.0-5.00.223-beta but does not work on true 5.0 version. and it has a bug in 3.31. At least one variant works under 5.0 With virus not active in memory, CHKDSK reports many cross-linked files and lost file chains, and copied infected files are only 1024 bytes long or the size one 1 cluster, usually 1 K; backups disks and other full disks can become corrupted when virus writes to the last cluster.
With virus not active in memory, CHKDSK -F or Norton Disk Doctor will destroy most executible files on the disk.

Detect with: DDI Data Physician V 3.0B, McAfee's CLEAN v84, Microcom's VIRx 1.8, F-PROT 2.01, Dr. Solomon's Anti-virus Toolkit V 5.13, Manual method described below.
These 4 detection steps are independant of each other:
1. Boot from a known clean floppy and run CHKDSK with no parameters. An indication of infection is a report of many cross-linked files and lost file chains.
2. WITH VIRUS ACTIVE IN MEMORY, perform a DIR. Now boot from a known clean floppy and perform a DIR. If the size of executible files changes between the two, it is fairly certain the virus is present.
3. With virus ACTIVE in memory, try to delete a file from a write protected diskette. If you don't get an error message, it is a sign of infection.
4. Format a new diskette and look at its map with PC Tools. If one cluster of the diskette is allocated (not bad) and it is at the end of the diskette, then it is probable the virus is resident and active in memory DDI Data Physician V 3.0B, McAfee's CLEAN v84, Bontchev's DIR2CLR
Use this 5-step process (Anti viral program versions prior to October 1991 are inadequate to find/eradicate this virus: 1. With DIR II active in memory, use the COPY command (RENAME command may also work, but COPY is more definitive) to copy all .EXE and .COM files to another file with a different extension. Example COPY file.EXE file.VXE
2. Reboot system from a clean, write protected diskette to ensure the system does NOT have the virus in memory. 3. Delete all files with extensions of .EXE and .COM. This will remove all pointers to the virus.
4. Rename all executibles to their original names. Example RENAME file.VXE file.EXE
5. Examine all these executibles you have just restored with the DIR command. if any are 1K in length, they are probably a copy of the virus and must be destroyed.
After eradication it may be desirable to now run CHKDSK /f or another disk optimization utility to ensure the virus is no longer anywhere on the disk.

Name: Disk Killer		
Aliases: Disk Killer, Computer Ogre, Disk Ogre	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorInterferes with a running application.Corrupts a program or overlay files.Corrupts a data file.Encrypts the data on the disk.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Infects floppy and hard disk boot sectors and after 48 hours of work time, it displays the following message Disk Killer -- Version 1.00 by COMPUTER OGRE 04/01/1989 Warning !! Don't turn off the power or remove the diskette while Disk Killer is Processing! PROCESSING It then encrypts everything on the hard disk. The encryption is reversable. Word at offset 003Eh in the boot sector will contain the value 3CCBh.		

Name: DISKSCAN		
Aliases: DISKSCAN, SCANBAD, BADDISK	**Type:** Trojan.	
Disk Location: DISKSCAN.EXESCANBAD.EXEBADDISK.EXE	**Features:**	
Damage: Overwrites sectors on the Hard Disk.	**Size:**	**See Also:**
Notes: This was a PC-MAGAZINE program to scan a [hard] disk for bad sectors, but then a joker edited it to WRITE bad sectors. Also look for this under other names such as SCANBAD.EXE and BADDISK.EXE. A good original copy is availble on SCP Business BBS.		

Name: Diskspoiler		
Aliases: Diskspoiler	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 1308	**See Also:**
Notes:		

Name: Dismember		
Aliases: Dismember	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 288	**See Also:**
Notes:		

Name: DM		
Aliases: DM, DM-310, DM-330	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 400310330	**See Also:**
Notes: The virus contains the following text: (C)1990 DM		

Name: DMASTER		
Aliases: DMASTER	**Type:** Trojan.	
Disk Location: DMASTER.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This is yet another FAT scrambler.		

Name: Do Nothing		
Aliases: Do Nothing, Stupid Virus, 640K Virus	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 583	**See Also:**
Notes: Infects .COM files. The virus copies itself to 9800:100h, which means that only computers with 640KB can be infected. Many programs also load themselves to this area and erase the virus from the memory.		

Name: Doom		
Aliases: Doom, Doom II, Doom-2B	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.	
Damage:	**Size:** 1252	**See Also:**
Notes: virus-l, v4-131 says that a variant of the 512 and Doom-II virus can put executable code into video memory. The virus code contains the text, DOOM II (c) Dr.Jones, NCU.		

Name: Doomsday		
Aliases: Doomsday, Null Set, Scion	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 733	**See Also:**
Notes: The virus contains the following texts, A scion to none Certainly no fun Total destruction when done Introducing DOOMSDAY ONE Written in Orlando, FL on 05/13/91 Your disk is dead! Long live DOOMSDAY 1.0		

Name: Dos 7		
Aliases: Dos 7	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and removeDos 7 (342, 376, 419)		

Name: DOS-HELP		
Aliases: DOS-HELP	**Type:** Trojan.	
Disk Location: DOS-HELP.???	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: This trojan, when made memory-resident, is supposed to display a DOS command for which the User needs help with. Works fine on a Diskette system but on a HARD DRIVE system tries to format the Hard Disk with every access of DOS-HELP.		

Name: DOShunt		
Aliases: DOShunt	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Trashes the hard disk.	**Size:** 483	**See Also:**
Notes: Activates on June 26 and trashes the hard disk.		

Name: DOSKNOWS		
Aliases: DOSKNOWS	**Type:** Trojan.	
Disk Location: DOSKNOWS.EXE	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 5376 Size of the real DOSKNOWS.EXE	**See Also:**
Notes: Apparently someone wrote a FAT killer and renamed it DOSKNOWS.EXE, so it would be confused with the real, harmless DOSKNOWS system-status utility.		

Name: Dosver		
Aliases: Dosver	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Doteater		
Aliases: Doteater, Dot Killer, Point Killer	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Interferes with a running application.	**Size:** 944	**See Also:**
Notes: When activated, it removes all dots from the screen. All periods disappear from the screen. v6-151: At least one anti-virus program can detect and remove Doteater (C, D and E).		

Name: DPROTECT		
Aliases: DPROTECT	**Type:** Trojan.	
Disk Location: DPROTECT.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Apparently someone tampered with the original, legitimate version of DPROTECT and turned it into a FAT-table eater. A good version is available on SCP Business BBS.		

Name: Dracula		
Aliases: Dracula	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Dragon		
Aliases: Dragon	**Type:** Other: Parasitic file infector	
Disk Location: EXE application.	**Features:** Memory resident; TSR.StealthFast infector type	
Damage: Corrupts some EXE files which causes system crashNo damage, only replicates.	**Size:** Overlays application, no increase	**See Also:**

Notes:
The following text extracted from VB March 1995:
This virus non standard method in intercepting and infecting EXE file. It hooks Int 13h vector to control disk access and test for EXE stamp 'MZ'. The virus needs 400 byte for its code and data. The virus inserts itself in EXE header and modifies the header so that control is passed to the virus upon the execution. The execution of an infected file will trigger the installation routine in system memory. The installation routine will allocate 400 bytes at the top of base memory and marks the MCB owner filed as 'system' and copies itself at that block. The size, location, and stealth technique of this virus makes the virus hard to detect as well as allowing for fast infection.

Once the virus is a memory resident, it obtains the DOS Data Table pointer using Get List Of List and searches for Drive Parameter Blocks for both floppy and hard disks drivers. The virus stores the address of Strategy and Interrupt handler of any such driver, then it sets its own address as the original device driver. Thus, any DOS call to the drivers will be passes to the virus, the virus performs its function, then calls the original device driver.

The virus code is build on the assumption that most EXE header have an unused space padded with zero up to a maximum of 480 bytes. It designed to write itself between offset 0070h and 0200h in the header. When that location of the EXE header has other information and instruction, then they will be lost upon the infection and the EXE file is corrupted. The execution of a corrupt EXE file will cause a system crash.

Note:
Dragon may have problems working under NetWare and in multitasking environment.

The removal should be done under clean system conditions. The infected files should be identified and replaced. The Hex Pattern of the virus in files and in memory is as follows:

```
8CC8  2E01  0691  000E  0606  8CC0
488E  C026  8E1E  0300  83EB  1A07
```

Name: DRAIN2		
Aliases: DRAIN2	**Type:** Trojan.	
Disk Location: DRAIN2.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: There really is DRAIN program, but this revised program goes out does Low Level Format while it is playing the funny program.		

Name: DROID		
Aliases: DROID	**Type:** Trojan.	
Disk Location: DROID.EXE	**Features:**	
Damage:	**Size:** 54272 Size of DROID.EXE	**See Also:**
Notes: This trojan appears under the guise of a game. You are supposedly an architect that controls futuristic droids in search of relics. In fact, PC-Board sysops, if they run this program from C:\PCBOARD, will find that it copies C:\PCBOARD\PCBOARD.DAT to C:\PCBOARD\HELP\HLPX.		

Name: Dropper7		
Aliases: Dropper7, Dropper 7	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.Stealth; actively hides from detection.	
Damage:	**Size:**	**See Also:** Dropper7 Boot
Notes: Can not be removed. Infected files must be deleted.		

Name: Dropper7 boot		
Aliases: Dropper7 boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.Stealth; actively hides from detection.	
Damage:	**Size:**	**See Also:** Dropper7
Notes:		

Name: DRPTR		
Aliases: DRPTR, WIPEOUT	**Type:** Trojan.	
Disk Location: DRPTR.???	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**
Notes: After running unsuspected file, the only things left in the root directory are the subdirectories and two of the three DOS System files, along with a 0-byte file named WIPEOUT.YUK. COMMAND.COM was located in a different directory; the file date and CRC had not changed.		

Name: DSZBREAK		
Aliases: DSZBREAK	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Not sure if virus or trojan (v5-031) A program supposedly meant to break the registration requirement on Omen Software's DSZ (zmodem protocol). It works on some kind of a timer, so when you leave your machine running without using the keyboard, it will then make anything you attempt to enter from the keyboard a control character (DIR would become ^D^I^R). It appears to live in the boot sector, as reloading your .sys files fack to your dos directory or reformatting C: will get rid of it.		

Name: Du		
Aliases: Du	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Dudley		
Aliases: Dudley, odud, Oi Dudley	**Type:** Program.	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:**	**See Also:**
Notes: v6-140: First - Dudley is polymorphic....no signatures are possible. Second, the virus is not very new, and many scanners will detect it without problems... at least the current F-PROT does. - -frisk v6-142: reported first in Australia		

Name: Durban		
Aliases: Durban, Saturday the 14th	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Saturday 14th.B.		

Name: Dutch Tiny		
Aliases: Dutch Tiny, Dutch Tiny-124, Dutch Tiny-99	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 12612499	**See Also:**
Notes:		

Name: Dy		
Aliases: Dy	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Dzino		
Aliases: Dzino	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: E. T. C.		
Aliases: E. T. C.	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** 700	**See Also:**
Notes: The virus contains the text, E.T.C. VIRUS, Version 3.0, Copyright (c) 1989 by E.T.C. Co.		

Name: E-Rillutanza		
Aliases: E-Rillutanza, Rillutanza	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Ear		
Aliases: Ear, Quake, Suicide	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 1024960 - Quake variant2048 - Suicide variant	**See Also:**
Notes: The virus asks questions about the anatomy of the ear.		

Name: Eastern Digital		
Aliases: Eastern Digital	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1600	**See Also:**
Notes: The virus contains the text, MegaFuck from Eastern Digital It may affect Backup.com		

Name: Eddie 2		
Aliases: Eddie 2	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 651	**See Also:**
Notes: Similar to the Eddie virus, it contains the string, Eddie Lives The seconds field of the time stamp contains 62. The virus hides its length change by trapping the DIR command and adjusting the length of any file with 62 in the seconds field of the time stamp.		

Name: EDV		
Aliases: EDV	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** brain
Notes: Derivative of Brain, with the eighth bit set, using the ISO 8859-1 character table it will result in the swedish/finnish national characters in their major form and in alphabetical order. (virus-l, v5-73). This is just a coincidence, in the the EDV virus is French.		

Name: EDV		
Aliases: EDV, Cursy	**Type:** Boot sector.Activates once at boot time.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage:	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: This virus hides in the upper memory block in any free memory below E800. It also issues a HLT instruction if ES or DS is pointing to it (indicating it is being scanned). The end of the boot sector contains the text EV. On a 360 K disk, the original boot sector is in the last sector of the last track. Contains an encrypted text string, That rings a bell,no ? from Cursy		

Name: EGABTR		
Aliases: EGABTR	**Type:** Trojan.	
Disk Location: EGABTR.???	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**
Notes: BEWARE! Description says something like "improve your EGA display," but when run, it deletes everything in sight and prints, "Arf! Arf! Got you!"		

Name: Eight Tunes		
Aliases: Eight Tunes, 1971, 8-Tunes	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1971-1986 .COM applications bytes: (length -3) mod 16 = 0.1971-1986 .EXE applications bytes: (length -3) mod 16 = 0.	**See Also:**
Notes: During load procedure, .COM and .EXE files are infected. 90 days after the infection, after 30 minutes, the virus will play one of eigth melodies (random selection). After a short time, the virus will play a melody again. The virus looks for and deactivates "BOMBSQAD.COM", an antivirus-tool controlling accesses to disks. The virus looks for "FSP.COM" (Flushot+), an antivirus tool controlling accesses to disks, files etc., and stops the infection if it is found. Your computer is randomly playing short tunes. Typical texts in Virus body (readable with HexDump-facilities):"COMMAND.COM" in the data area of the virus .Com files: the bytes 007h,01fh,05fh, 05eh,05ah,059h,05bh,058h,02eh,0ffh,02eh,00bh, 000h are found 62 bytes before end of file . .EXE files: the bytes 007h,01fh, 05fh,05eh,05ah,059h,05bh,058h,02eh,0ffh,02eh, 00bh,000h are found 62 bytes before end of file.		

Name: Eliza		
Aliases: Eliza	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 1193-1194 TO COM filesDestroys .EXE files	**See Also:**
Notes: Infected .COM files do not replicate. Infected .EXE files are destroyed. Lots of bugs in this virus.		

Name: EM		
Aliases: EM	**Type:** Program.	
Disk Location: EXE application.	**Features:** EncryptedDirect acting.Infects files on C: drive only!	
Damage: Corrupts system sector containing file directory entry.Corrupts a program or overlay files.	**Size:** 1303 bytes long.	**See Also:**

Notes:
The following notes are extracted from VB, July 1995:

EM is 1303 bytes long, encrypted virus that appeared in Russia.

The virus has two forms. The first form is a 1303 byte file called EM.COM which a COM file and its executed whenever DOS processes AUTOEXEC.BAT at load time. The second form is the usual EXE file appender.

The EM.COM is activated each time the system is booted. The first activity is to check the date, and if the date is 28 th, then the trigger routine is activated, otherwise it infects 10 EXE file on C: drive. On every reboot, EXE files are infected until all are infected.
On the 28th day on any month, EM delivers its payload. The virus scans the subdirectory tree of the C: drive, then it obtains the address of subdirectories, and finally corrupts each entry name. It overwrites the name of each entry with a 'SPACE' character (Data inside the file are not changed). The result is that DOS can not access these entries, since DOS does not support the space character in names. Using DIR command all entries are displayed with 'SHORTENED NAME'.

Restoring data files with corrupt names should be simple, just using the 'RENAME ' command. The AUTOEXEC.BAT file should be cleaned by removing the line the contains 'em' (i.e. preventing EM.COM from execution by DOD). As for the EXE files, they must be identified and replaced under clean system condition.

For more info about the EM virus, read the VB article about this particular virus.

Name: EMF		
Aliases: EMF	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 404625	**See Also:**

Notes: The virus contains the text,
Screaming Fist
The screamer virus also contains this text, possibly indicating that they were written by the same author.

Name: Emma		
Aliases: Emma	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.Hides in EMS (expanded memory blocks).	
Damage: No damage, only replicates.Unknown yet.	**Size:** 427 byte long.Appending parasitic COM file infector.	**See Also:**

Notes:
Emma is 427 byte long. It is appended to COM files with a JMP instruction at the start of the infected COM file.

The infection process of EMS starts with the executing an infected file. The JMP passes control to the virus code, which test system memory for an active copy of itself. If an active copy is found then the control is returned to the host program; otherwise the virus attempts to install itself into system memory using Int 67h handler. The first step is to determine whether the EMS driver is loaded. If no driver is found, then control is returned to host file and system memory is not infected. If an EMS driver is found, then the virus obtains the number of unallocated pages. Control is passed to the host file when no free pages are found. Otherwise, the virus finds the EMS frame segment address and stores it. Then, it allocates one EMS page and makes it available for its use. Then it copies itself into that frame and unmaps the page. Now, the virus is stored in EMS memory. The rest of the installation routines are : 1) to copy the virus' Int 21h into the Interrupt Vector Table at address 0024:0000h which is the same address as the virus ID word. 2) to hook Int 21h. Finally, control is returned to the host program.

Files are infected when they are executed on an infected system memory. The main code of the virus takes control over the file. First, it makes sure that the DOS function is Load_and_Execute. If so then it allows the original the process to complete, then the virus attempts to infect the file. It opens the file and read the header, if the first instruction is a JMP instruction, it calculates the offset. If the jump is 430 byte from the end file, then it assumes that the file is infected and control is returned to the calling function. If the header is not JMP instruction, then the virus checks for EXE and COM stamps. If the file is and EXE type, then the infection routine is aborted, otherwise it appends its body to the end file and modified the header to JMP VIRUS instruction, then it returns control to the calling code.

Detection and removal of the virus should be easy. Emma writes it ID word 2E9CH at the address 0024:0000h of the system memory and its Int 21h code are inserted in the Interrupt Vector Table. Virus scanner should detect these changes without scanning EMS memory. The virus is removed from memory by removing the EMS driver from CONFIG.SYS, next rebooting the computer. Infected files can be identified and removed under clean system condition.

Name: Emmie		
Aliases: Emmie	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 2702	**See Also:**
Notes:		

Name: Empire		
Aliases: Empire, Empire A, Empire C, Empire D, Stoned variant, Empire B.2, UofA	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Azusa
Notes: Derived from the Stoned virus, originally from Univ. of Alberta. Last known variant released July 10, 1991, total of 18 variants identified to date. Variants have differences in the code, indicating separate prramming efforts on the part of the virus writer. Empire C gets around the simple "chkdsk" for boot sector viruses. Since most boot sector viruses have to reduce the number of "total bytes of memory" of a computer to hide at the top of memory, the virus can be detected by seeing whether "chkdsk" returns 1k or 2k less than it is supposed to return. Empire C didn't bother telling DOS that the virus was present in memory when it installed itself. It puts itself at 9000:0000 or 80000:0000 and functioned until something else used that memory location, then the system crashed. Empire D was a response to an installation of "Disk Secure". It recognized the presense of Disk Secure and removes it before infecting the computer. These are the most common viruses at the Univ. of Alberta and in Edmonton. See also listing for Empire B.2, or UofA virus McAfee Scan v80 may detect some Empire strains as Azusa		

Name: Empire B.2		
Aliases: Empire B.2, UofA, derived of Stoned	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Contains a data diddler routine. On any write to a floppy, the virus may randomly decide to alter one or more bytes being written, to a new random value. This variant does not announce its existence in any way. Does not use stealth, and can be detected using several virus scanners. Uses 1k of memory from "top of memory" and it tends to not work with 720k diskettes, they appear unreadablebecause DOS thinks they are 1.2Mb.		

Name: Encroacher		
Aliases: Encroacher	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: will search for and delete these CPAV files: CHKLIST.CPS, CPAV.EXE, and VSAFE.COM		

Name: End of		
Aliases: End of	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes:		

Name: Enola		
Aliases: Enola	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 18642430	**See Also:**
Notes:		

Name: EUPM		
Aliases: EUPM, Year 1992, Apilapil	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Trashes the hard disk.	**Size:** 1731	**See Also:**
Notes: If the year is set to 1992, it overwrites the hard disk. v6-151: At least one anti-virus program can detect and remove Year 1992.B.		

Name: Europe '92		
Aliases: Europe '92, Dutch 424	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 421	**See Also:**
Notes: If the year is set to 1992, it displays the message, Europe/92 4EVER!		

Name: EXEBUG		
Aliases: EXEBUG, EXEBUG1, EXEBUG2, EXEBUG3, exe_bug	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR above TOM.Stealth	
Damage: Corrupts hard disk partition table	**Size:** 512 bytes	**See Also:**

Notes: One report said that it overwrites random sectors in March. On some systems, it can appear that this virus can survive a cold boot (see posting included below).

From a posting in alt.comp.virus, 2/95:
"Exebug is a memory resident infector of floppy diskette boot sectors and hard disk master boot records. The original boot sectors will be stored in encrypted form elsewhere on the disk, depending on the disk type. And the disk boot sector will now be replaced by the viral boot sector which will not be a legal MBR! It is a very complicated virus. If you are infected with Exebug, all attempts to read the boot sector will be redirected to the correct version of the boot sector. As a result, your system will seem to be unaffected. The only way to detect the virus when infected is by its memory signature.

Exebug steals 1K of memory from the 640K mark. Thus infected systems will show 1K less memory available than normal. The virus will alter the CMOS configuration of the system to report that there is no A: drive. On some systems, this alteration causes the system to always boot first from the C: drive. Thus, on those systems, the virus will get into memory first. The virus, understanding that a user just attempted to reboot, will then simulate the booting process from A: but it will already be in memory.

Apart from these technical complications, the virus does not intentionally damage the computer. Sector 7 of the hard disk boot track or a sector on track 0 of floppies is used to store the original boot sector. Thus, it might overwrite information."

Name: F-Soft		
Aliases: F-Soft, Frodo Soft, F-Soft 563	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 458563 - F-Soft 563 variant	**See Also:**
Notes: The virus contains the text , (c) Frodo Soft The 563 variant is encrypted.		

Name: F-Word		
Aliases: F-Word, Fuck You, F-you	**Type:** Program.	
Disk Location: COM application.EXE application - 593 and 635 variants	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 417593635	**See Also:**
Notes: The virus contains the text, Fuck You		

Name: F1-337		
Aliases: F1-337	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 337	**See Also:**
Notes:		

Name: Faerie		
Aliases: Faerie	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 276 bytes	**See Also:**
Notes: The last sector of the .COM file contains the word FAERIE. It doesn't infect COMMAND.COM.		

Name: Fax Free		
Aliases: Fax Free, Mosquito, Topo, Pisello	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: EXE application.	**Features:** EncryptedDirect acting.	
Damage: Unknown, not analyzed yet.	**Size:** 10241536	**See Also:**
Notes: The virus contains the following text: Hello this is the core Rev 3 26/4/91 P 0.98c P. 0.98 Rev 4 24IX89 bye bye		

Name: FCB		
Aliases: FCB	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase 384 bytes long	**See Also:**
Notes: Delete infected files		

Name: Feist		
Aliases: Feist	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 670	**See Also:**
Notes:		

Name: Fellowship		
Aliases: Fellowship, Better World	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1019	**See Also:**
Notes: The virus contains the text: This message is dedicated to all fellow PC users on Earth Towards A Better Tomorrow And A Better Place To Live In The virus is actually not very friendly		

Name: FGT		
Aliases: FGT	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 651	**See Also:**
Notes:		

Name: Fichv		
Aliases: Fichv, Fichv-EXE 1.0	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application Fichv-EXE 1.0 variant	**Features:** EncryptedDirect acting.	
Damage: Overwrites sectors on the Hard Disk.	**Size:** 903897 Fichv-EXE 1.0 variant	**See Also:**
Notes: The virus contains the text ***FICHV 2.1 vous a eu***** When activated, it overwrites the first 6 sectors of the track 0, head 1 of the current drive.		

Name: Filedate 11		
Aliases: Filedate 11, Filedate 11-537	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 570537 - variant	**See Also:**
Notes:		

Name: FILES.GBS		
Aliases: FILES.GBS	**Type:** Trojan.	
Disk Location: FILES.GBS	**Features:**	
Damage: Bypasses OPUS BBS's security.	**Size:**	**See Also:**
Notes: When an OPUS BBS system is installed improperly, this file could spell disaster for the Sysop. It can let a user of any level into the system. Protect yourself. Best to have a sub-directory in each upload area called c:\upload\files.gbs (this is an example only). This would force Opus to rename a file upload of files.gbs and prevent its usage.		

Name: Filler		
Aliases: Filler	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The virus code and the original boot sector are hidden on track 40, outside of the normal range of tracks. v6-139: doesn't think that this obscure Hungarian boot sector virus is in the wild. Some false alarms have occurred with old versions of CPAV.		

Name: Finnish		
Aliases: Finnish, Finnish-357	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 709	**See Also:**
Notes: The virus infects every .COM file run, or opened for any reason. v6-151: At least one anti-virus program can detect and remove Finnish.709.C		

Name: Fish		
Aliases: Fish, European Fish,Fish 6	**Type:** Program.Encrypted/Stealth The virus actively hides. Boot Sector	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.Corrupts a data file.	**Size:** 3584	**See Also:**
Notes: If (system date>1990) and a second infected .COM file is executed, a message is displayed: "FISH VIRUS #6 - EACH DIFF - BONN 2/90 '~Knzyvo}'" and then the processor stops (HLT instruction). The virus will attempt to infect some data files, corrupting them in the process. This is a variant of the 4096 virus. There is another virus named FISH that is a boot sector virus. (kp 2/26/93)		

Name: Flash		
Aliases: Flash, 688, Gyorgy	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 688	**See Also:**
Notes: The memory resident virus infects applications when they are run. After June 1990, the virus makes the screen flash. This flash can only be seen on MDA, Hercules, and CGA adapters, but not on EGA and VGA cards. The Gyorgy variant contains the text "I LOVE GYÖRGYI". A flashing screen.		

Name: Flip		
Aliases: Flip, Omicron, Omicron PT	**Type:** Boot sector.	
Disk Location: COM application.EXE application.Hard disk boot sector.	**Features:** Polymorphic	
Damage:	**Size:** 2153 and 2343 strains existPolymorphic: each infection different/some strains	**See Also:**
Notes: Multi-partite virus. (infects both boot sectors and files) FProt finds Flip on two files of Central Point Anti-Virus: this is a false positive. The 2343 strain (the rarer one) patches COMMAND.COM 2nd Day of every month activates on a system with an EGA or VGA display between 1600 and 1659 and reverses the screen and characters.		

Name: Flower		
Aliases: Flower	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 883	**See Also:**
Notes: This virus activates on Nov. 11th. Any infected file run on that date is overwritten wit a Trojan that displays the following text: FLOWER Support the power of women Use the power of man Support the flower of woman Use the word FUCK The word is love		

Name: FLUSHOT4		
Aliases: FLUSHOT4, FLU4TXT	**Type:** Trojan.	
Disk Location: FLUSHOT4.ARC	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This Trojan was inserted into the FLUSHOT4.ARC and uploaded to many BBS's. FluShot is a protector of your COMMAND.COM. As to date, 05/14/88 FLUSHOT.ARC FluShot Plus v1.1 is the current version, not the FLUSHOT4.ARC which is Trojaned.		

Name: Forger		
Aliases: Forger	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a data file.	**Size:** 1000	**See Also:**
Notes: Corrupts data when it is written to disk.		

Name: Form		
Aliases: Form, Form Boot, FORM-Virus, Forms	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.Bad blocks.Or at end of physical drive in unused sectors.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts a program or overlay files.Deletes or moves files.	**Size:** Overlays boot sector, no increase	**See Also:**

Notes: A boot sector virus that randomly destroys files. Dual acting; Attempts to infect the hard disk at boot time. Attempts to infect a floppy whenever the floppy is read.
Does not infect the Master Boot Record (Partition table), but the boot record of the first logical drive (C:). It is also marks a cluster as bad, and stores the rest of the virus there.
On the hard disk, if there are some left over sectors at the end of the physical drive that are not part of a cluster (not enough sectors to fill a cluster). The virus hides there. In memory, the virus goes resident and moves down the TOM by 2K. (wjo 11/94)
The command FDISK/MBR is ineffective against FORM because it is not in the MBR (v5-190)
Versions of FPROT prior to 2.06a can't remove the virus.
The SYS command removes the virus by rewriting the disks boot sector. It does not remove the part stored in the bad sector or at the end of the drive, but that part won't hurt anything without the part in the boot sector.
The virus makes the keys click and delays key action slightly. The keys don't start clicking as soon as the machine is infected.
The boot sector will contain the following text(amongst others):
"The FORM-Virus sends greetings to everyone who's read this text.".
To remove it, boot from a clean disk and rewrite the boot sectors of an infected disk with the SYS command. Repeat for all infected disks.
May have been on demo diskette of Clipper product. (virus-l V4-213)
(Dave Chess, V6-106): There are some viruses that will infect whatever partition is currently marked bootable, regardless of whether or not it's a DOS partition. The FORM virus is particularly inept in this regard: it will infect whatever's marked bootable, and it will assume that the partition it's infecting is a FAT-formatted partition for purposes of finding unused space to hide itself. This can wreak havoc when the bootable partition is actually BootManager or HPFS, for instance.

Name: Freddy		
Aliases: Freddy	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1870	**See Also:**

Notes: The virus contains the text, Freddy Krg
Nov 92, virus-l v5-188: CLEAN v97 and v99 may have trouble disinfecting Freddy, reports that Jeru virus was found. Clean corrupted the files, which hung user's computer.
Since its not a Jer. variant, that won't work. Freddy appends itself to .COM files, DOESN'T add it's code to the beginning.

Name: Free Agent		
Aliases: Free Agent, timer	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: The following bogus message was distributed to several news groups. It claims that the Free Agent program from Solomon has a time bomb. Solomon claims this is false.

- ---------- Forwarded message ----------
Date: Fri, 02 Feb 1996 09:59:57 -0500 (EST)
From: Managing Director <Dr.Solomon@de.drsolomon.com>
To:
Subject: Free-Agent - timer Virus!! ALERT!! Serious threat..

02 February 1996 - Bullitin Report.

Please read the following and take it very seriously.

During the designe stages of the beta version of Free-Agent, an employee was sacked for steeling company property. Until yesterday no nobody knew that the person in question had logged into the main computer on the night that he had been sacked, he changed the coding within Free-Agent so that on the 01st February 1996 a time bomb would go off. Anybody using Free-Agent has already been infected.

THIS IS SERIOUS::::::::

In order to clean your hard disk of this virus you must first do a low level format. Then make sure any disks you have used since yesterday are destroyed as we currently have no cure for this virus, it is a very advanced polymorphic virus with a Trojan side affect, meaning that it will copy itself only once per disk, after that it waits until you switch of you PC and when you turn on again, it is to late the Virus has already infected your DBR and MBR, if left to long it will destroy your Partition sectors and you will have no choice but to destroy the disk. A low level format after this will result in an error unable to format hard disk. If the information stored on your disk is very valuable then we do a data recovery service, you can ring us on +44 (0) 1296 318733 UK.. Or e-mail myself directly, I will respond as soon as I can.

If you have only switched on and did not use the computer yesterday, then do this:- Remove your copy of Free-Agent and do virus recovery procedure as laid out in your anti-virus manual.

This is a serious threat and could cost business thousands of dollars, unless you act fast.. REMEMBER: Low level Format then Destroy used floppies. Hopefully you will all have made backups of your software. Just remember not to reload your original copy of Free-Agent. Forte are currently decoding the software and promise me they will have it on the net at 18:00hrs tonight GMT

- ------- End of Forwarded Message

Name: Freew		
Aliases: Freew	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 692	**See Also:**
Notes: Overwrites files with a Trojan that prints "Program Terminated Normally" when run.		

Name: Friday 13 th COM		
Aliases: Friday 13 th COM, South African, 512 Virus, COM Virus, Friday The 13th-B, Friday The 13th-C, Miami, Munich, Virus-B, ENET 37	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 419613 - ENET 37 variant	**See Also:** number of the beast, Compiler.1, Darth Vader
Notes: Infects all .COM files except COMMAND.COM, and deletes the host program if run on Friday the 13th. Beast: SCAN 97 still says that "number of the beast" is the 512 virus, also says that Compiler.1 and Darth Vader viruses are also 512 virus (erroneously) Files disappear on Friday the 13th. Text "INFECTED" found near start of virus. v6-151: At least one anti-virus program can detect and remove Friday the 13th (540.C and 540.D)		

Name: Frog's Alley		
Aliases: Frog's Alley	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: reported in Virus-l, v4-255, no more info		

Name: Frogs		
Aliases: Frogs, Frog's Alley	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1500	**See Also:**
Notes: Files are infected when a DIR command is executed. The file contains the following encrypted text. AIDS R.2A - Welcome to Frog's Alley !, (c) STPII Laboratory - Jan 1990..		

Name: Fu Manchu		
Aliases: Fu Manchu, 2086, 2080, Fumanchu	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 2086 Increase of .COM files2080-2095 Increase of .EXE files length mod 16 equals 0	**See Also:** Jerusalem, 1813
Notes: Infects .COM and .EXE files. The message 'The world will hear from me again! ' is displayed on every warmboot, and inserts insults into the keyboard buffer when the names of certain world leaders are typed at the keyboard. Occasionally causes the system to spontaneously reboot. Deletes certain 4 letter words when typed at the keyboard.		

Name: Funeral		
Aliases: Funeral	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 921	**See Also:**
Notes: Plays a tune		

Name: FUTURE		
Aliases: FUTURE	**Type:** Trojan.	
Disk Location: FUTURE.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: This "program" starts out with a very nice color picture and then proceeds to tell you that you should be using your computer for better things than games and graphics. After making that point, it trashes your A: drive, B:, C:, D:, and so on until it has erased all drives.		

Name: G-MAN		
Aliases: G-MAN	**Type:** Trojan.	
Disk Location: G-MAN.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Another FAT killer.		

Name: GATEWAY		
Aliases: GATEWAY, GATEWAY2	**Type:** Trojan.	
Disk Location: GATEWAY.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Someone tampered with the version 2.0 of the CTTY monitor GATEWAY. What it does is ruin the FAT.		

Name: Geek		
Aliases: Geek	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 450	**See Also:**
Notes:		

Name: Gemand		
Aliases: Gemand	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Genb		
Aliases: Genb, genp, Generic Boot, GenericBoot, NewBug, New Bug	**Type:** Boot sector.	NOT ANY PARTICULAR VIRUS!!!
Disk Location: Hard disk boot sector.	**Features:**	
Damage:	**Size:**	**See Also:** Form, Brasil, AntiEXE

Notes: This is NOT a particular virus!

McAfee's SCAN program says identifies some boot sector viruses as the "genb" or "genp" viruses when it finds a suspicious scanning string in the boot sector . Viruses that have appeared that are identified as genb include FORM, AntiEXE and Brasil.
Virhunt uses the name Generic Boot.
CPAV uses the name New Bug.
Eradication may occur if you run SYS C:, but backup your hard disk first!

---
from virus-l, v6-104:
There is no such thing as "the Generic Boot Virus". What Scan means when it reports GenB, is that it has found a piece of highly suspicious code in the boot sector, but does not find a search string belonging to any known virus.

This can mean:

1) A new virus.
2) A false alarm, for example if the boot sector contains some obscure security program.
3) A damaged or partly overwritten copy of an old virus.

Determining exactly what is going on requires an analysis of the actual boot sector.

- -frisk

Name: Genc		
Aliases: Genc	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Genc (502 and 1000)		

Name: Gergana		
Aliases: Gergana, Gergana-222, Gergana-300, Gergana-450, Gergana-512	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 182	**See Also:**
Notes: The virus contains the text "Gergana", and "Happy 18th Birthday"		

Name: Ghost		
Aliases: Ghost	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts boot sectorCorrupts a program or overlay files.	**Size:** 2351	**See Also:**
Notes: Infects .COM files.		

Name: GhostBalls		
Aliases: GhostBalls, Ghost Boot, Ghost COM, Vienna, DOS-62	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts boot sectorInterferes with a running application.Corrupts a program or overlay files.	**Size:** 2351	**See Also:**
Notes: Variant of Vienna that puts a patched copy of the Ping Pong virus in the boot of drive A. It may infect floppy and hard disk boot sectors, sources differ on this. It contains the following text strings: GhostBalls, Product of Iceland Copyright (c) 1989, 4418 and 5F19 Bouncing ball on screen. COM files: "seconds" field of the timestamp changed to 62, as in the original Vienna virus. Infected files end in a block of 512 zero bytes. The string "GhostBalls, Product of Iceland" in the virus.		

Name: Girafe		
Aliases: Girafe, Trident, TPE	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** TPE
Notes: Contains the internal string "[MK / Trident]" v6-123: TPE.1_0.Girafe Disables Ctrl-Break checking		

Name: Gliss		
Aliases: Gliss	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1247	**See Also:**
Notes: Demonstration virus that announces its infections of programs.		

Name: Globe		
Aliases: Globe	**Type:** Program.DIET compressed	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 6610	**See Also:**
Notes:		

Name: Goga		
Aliases: Goga	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Gold_Bug		
Aliases: Gold_Bug, Gold Bug	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.	**Features:** StealthEncryptedPolymorphic	
Damage: Damages CMOS.	**Size:** Polymorphic: each infection different	**See Also:** Da'Boys
Notes: Gold_bug is a companion virus to Da'Boys. It hides Da'Boys during Windows startup by removing Da'Boys from the Int 13 startup chain and putting it back after Windows has started.		

Name: Goldbug		
Aliases: Goldbug	**Type:** Boot sector.	
Disk Location: Hard disk boot sector.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Infects MBR and 1.2MBoot sector, may remove itself on the next bootstrap and does nothing else Another report says that it replicates just fine, when first run, infects MBR, after a boot, it removed itself from the MBR but stayed in memory if there are UMBs available. Then it companion-infects EXE files under 64K that are executed. It refuses to run any exe file bigger than 64K that ends in "AN' - "AZ" (including scan, tbav, resscan) and messes up the CMOS if you do.		

Name: Golgi		
Aliases: Golgi	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Golgi (465 and 820)		

Name: Good Times		
Aliases: Good Times, GoodTimes, Good_Times, xxx-1	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage: Denial of service due to large numbers of e-mail messages warning others about the virus.	**Size:**	**See Also:**

Notes: " "Good Times" virus is an Urban Legend" from CIAC Notes 04c

In the early part of December, CIAC started to receive information requests about a supposed "virus" which could be contracted via America OnLine, simply by reading a message. The following is the message that CIAC received:

Here is some important information. Beware of a file called Goodtimes.

Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called "Good Times", DON'T read it or download it. It is a virus that will erase your hard drive. Forward this to all your friends. It may help them a lot.

THIS IS A HOAX. Upon investigation, CIAC has determined that this message originated from both a user of America Online and a student at a university at approximately the same time, and it was meant to be a hoax.

CIAC has also seen other variations of this hoax, the main one is that any electronic mail message with the subject line of "xxx-1" will infect your computer.

This rumor has been spreading very widely. This spread is due mainly to the fact that many people have seen a message with "Good Times" in the header. They delete the message without reading it, thus believing that they have saved themselves from being attacked. These first-hand reports give a false sense of credibility to the alert message.

There has been one confirmation of a person who received a message with "xxx-1" in the header, but an empty message body. Then, (in a panic, because he had heard the alert), he checked his PC for viruses (the first time he checked his machine in months) and found a pre-existing virus on his machine. He incorrectly came to the conclusion that the E-mail message gave him the virus (this particular virus could NOT POSSIBLY have spread via an E-mail message). This person then spread his alert.

As of this date, there are no known viruses which can infect merely through reading a mail message. For a virus to spread some program must be executed. Reading a mail message does not execute the mail message. Yes, Trojans have been found as executable attachments to mail messages, the most notorious being the IBM VM Christmas Card Trojan of 1987, also the TERM MODULE Worm (reference CIAC Bulletin B-7) and the GAME2 MODULE Worm (CIAC Bulletin B-12). But this is not the case for this particular "virus" alert.

If you encounter this message being distributed on any mailing lists, simply ignore it or send a follow-up message stating that this is a false rumor.

Name: Gosia		
Aliases: Gosia	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** Effective length of virus: 466 bytes	**See Also:**

Notes: Polish virus, first isolated in Poland in April 1991. It's rather primitive with logic similar to
W13. It only infects COM files. Infected files are marked by putting 44 in second field in file time stamp.

Not resident, does not use any stealth techniques. In one run it infects only 1 file in the current directory. COM files are recognized the extension of the name. It infects files with the length in the range
100-63,000 bytes. Write protected diskettes generate a write protect error.

Signature is: 5681C64401b90300BF0001FCF3A45E8BD6 - virus-l, v4-255
The name of the virus (Polish girl's nickname) is taken from a string inside the virus: "I love Gosia" where "love" is replaced by the heart character

This virus does not seem to contain any destructive code.

Name: Got You		
Aliases: Got You	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 3052	**See Also:**
Notes:		

Name: GOT319.COM		
Aliases: GOT319.COM	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 578 bytes	**See Also:**

Notes: No text is visible in the virus.
This virus appends to the end of files.

Name: Gotcha		
Aliases: Gotcha, Gotcha-D, Gotcha-E	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 879881906627 - Gotcha-D variant	**See Also:**

Notes: Contains the text,
GOTCHA!
Of Dutch origin probably (the comments are in Dutch, yes the virus came to the researcher with original source.)

Name: GRABBER		
Aliases: GRABBER	**Type:** Trojan.	
Disk Location: "GRABBER.COM"	**Features:** Memory resident; TSR.	
Damage: Deletes or moves files.	**Size:** 2583 Size of GRABBER.COM	**See Also:**
Notes: This program is supposed to be SCREEN CAPTURE program that copies the screen to a .COM file to be later run from a DOS command line. As a TSR it will attempt to do a DISK WRITE to your hard drive when you do not want it to. It will wipe out whole Directories when doing a normal DOS command. One sysop who ran it lost all of his ROOT DIR including his SYSTEM files.		

Name: Granada		
Aliases: Granada	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Green Caterpillar		
Aliases: Green Caterpillar, 1590, 1591, 1575, 15xx	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1575	**See Also:**
Notes: fairly widespread A green catapillar with a yellow head crawls across the screen, munching letters then shifting margins to the right.		

Name: Groen		
Aliases: Groen, Groen Links, Green Left	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Jerusalem
Notes: v6-151: At least one anti-virus program can detect and remove this Jerusalem variant		

Name: Grog		
Aliases: Grog, Lor	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Grog (Lor, 990 and d1641)		

Name: Groove		
Aliases: Groove	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Corrupts a data file.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Appears to be a mutation engine product that attacks anti-virus products by attacking their data files. v6-084: disables MSAV (MS DOS 6.0 antivirus program), targets checksum databases of some other products too (incl CPAV), the user may notice that something has happened. v6-122: will search for and delete these CPAV files: CHKLIST.CPS, CPAV.EXE, and VSAFE.COM		

Name: Grower		
Aliases: Grower	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 267+	**See Also:**
Notes: When it is run it infects all .COM programs in the current directory, with the length of the first one increasing by 268 bytes, the second by 269 bytes, the third by 270 and so on.		

Name: Grune		
Aliases: Grune	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.	**Features:** EncryptedDirect acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1241	**See Also:**
Notes: The virus contains the encrypted text: Arbeiten Sie jetzt wirklich umweltfreundlich ? Sie haben nun viel Zeit darüber nachzudenken ! Es grüsst Sie die "Grüne Partei der Schweiz" !		

Name: Gulf War		
Aliases: Gulf War	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This was a rumored virus that during the Gulf War there was a virus which would disable the enemy's computers. THIS VIRUS IS NOT REAL. IT IS A RUMOR.		

Name: Guppy		
Aliases: Guppy	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes: Only infects files that start with a JMP instruction. v6-151: At least one anti-virus program can detect and remove Guppy.D.		

Name: Gyro		
Aliases: Gyro	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 512Overlays application, no increase	**See Also:**
Notes:		

Name: Ha!		
Aliases: Ha!, Ha	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.	
Damage: Interferes with a running application.	**Size:** 1456	**See Also:**
Notes: Prints: ha! on the screen in large letters.		

Name: Haddock		
Aliases: Haddock	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 1355	**See Also:**
Notes:		

Name: Hafenstrasse		
Aliases: Hafenstrasse	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 809 - 1641	**See Also:** Ambulance
Notes: Some variants are droppers for the Ambulance virus.		

Name: Haifa		
Aliases: Haifa	**Type:** Program.loads itself to 8000:0100 (address fixed)	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Trashes the hard disk.Corrupts a data file.	**Size:** 2350 - 2400Polymorphic: each infection different	**See Also:**
Notes: This virus has no stealth capabilities and can be picked out quickly by using any directory listing program. Will not infect overlay, .BIN or .SYS files. couldn't get to spread on a 386 machine or when invoked on a floppy drive on any of 7 PCs. Prints out messages, and adds text to .DOC, .TXT, and .PAS files. Adds code to .ASM files that will overwrite the hard disk if assembled and run. When HAIFA infacts a file, it will set the minutes field of the time stamp to an even value (it clears the 0 but) and sets seconds field to 38; Unusual numbers of programs with seconds set to 38 are a possible indication of this virus.		

Name: Halloechen		
Aliases: Halloechen, Hello_1a, Hello, Halloechn	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a data file.	**Size:** 2011	**See Also:**
Notes: The virus slows the system down, and corrupts keyboard-entries (pressing an "A" produces a "B"). Does not infect files older than a month. The virus contains the text strings: "Hallöchen !!!!!!, Here I'm.. ", and " Acrivate Level 1.. " v6-151: At least one anti-virus program can detect and remove Halloechen (B and C)		

Name: Halloechen		
Aliases: Halloechen	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Halloechen (B and C)		

Name: Happy		
Aliases: Happy	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 412	**See Also:**
Notes: The virus contains the text: Thank you for running the Happy virus. Warning !!! COM-files in current directory and C:\DOS might be infected !!!!		

Name: Happy Days Trojan		
Aliases: Happy Days Trojan, HD Trojan	**Type:** Trojan.	
Disk Location: happyday.zip	**Features:**	
Damage: Deletes or moves files.	**Size:**	**See Also:**

Notes: The Happy Days trojan is being distributed via e-mail on America Online in the file happyday.zip around 2/1/96. It is supposed to improve the performance of a system. The distribution contains 4 files:

INSTALL.EXE
NECUSER3.TYE
README.TXT
RUNMENOW.COM

The Readme file contains the following text:

Hello, you are running Happy Days (R).
version 2.0
This program is a miracle b/c of its
size and its effectiveness. Run any
day, any time, and it increases your
productivity on the computer. Now we
all know how unproductive our sessions
at the computer can be, and this nifty
program will cure them all. Have a
Happy Day! with Happy Days (R) v2.0.

RUN the file RUNMENOW.COM in DOS only!!

If you run the runmenow.com file it displays the following text:

This program is this ultimate in home entertainment.
The magic of it is that it takes up minimal room on your harddrive,
and it doesn't use any precious RAM.
This file, RUNMENOW.COM, and its corresponding file INSTALL.EXE
work together. Remember, this file is universal and is great to use.
See README.TXT for documentation.
MAKE SURE YOU ARE IN DOS BEFORE RUNNING!!
Strike any key when ready...
Running Happy Day (R) v2.0...

The runmenow.com file runs install.exe which copies itself to the root directory of your C: drive and deletes files in the \dos, \windows and \windows\system directories. The Trojan tries to execute some other DOS commands, but they fail because it has already deleted the contents of the \dos directory.

Name: Happy Halloween		
Aliases: Happy Halloween	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 10,000	**See Also:**
Notes: Non resident, required minimum file size to infect, discovered Dec 1991 in British Columbia, CANADA File infects on exection, appears to seek out single file for infection of length greater than xxxx bytes. Infected files grow by 10,000 decimal bytes. Virus infects all files as if .exe - infected .com files will not execute properly. Virus may have at one time been compressed with LZEXE. Embedded string ("All Gone") indicates file deletion/destruction may occur on Oct 31 of any year after 1991 or Dec 25. COMMAND.COM infection will make floppy boot necessary. not found by common scanners. string: 6c6c6f7765656e55		

Name: Happy Monday		
Aliases: Happy Monday	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** varies	**See Also:**
Notes: A series of badly written companion viruses.		

Name: Happy New Year		
Aliases: Happy New Year, Bulgarian, Nina-2	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Unknown, not analyzed yet.	**Size:** 1600Command.com is overwritten	**See Also:**
Notes: Older virus (from around 1989 or 1990), this one was the first with the ability to infect device drivers, although it wasn't so easy to force it to infect them. Contains the text: "Dear Nina, you make me write this virus; Happy new year! " v6-151: At least one anti-virus program can detect and remove Nina (B and C)		

Name: Harakiri		
Aliases: Harakiri	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 5488 Overwriting	**See Also:**
Notes: Appears to have been written in Compiled Basic		

Name: Hary Anto		
Aliases: Hary Anto	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 981	**See Also:**
Notes:		

Name: Hate		
Aliases: Hate, Klaeren	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 974978 - 1000	**See Also:**
Notes: Because of an error, destroys programs larger than 4K bytes. The virus contains the encrypted string: "Klaeren Haß, Haß! " Note: Haß it "Hate" in German Named after a teacher in a school in Germany Slightly stealth, as it hides the date May NOT infect COMMAND.COM		

Name: Hates		
Aliases: Hates	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Headcrash		
Aliases: Headcrash	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Headcrash.B.		

Name: Helloween		
Aliases: Helloween	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 13761182	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Helloween (1227, 1384, 1447, 1839, 1888 and 2470)		

Name: Hero		
Aliases: Hero, Hero-394	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 506394	**See Also:**
Notes: Buggy virus that usually damages files while infecting them.		

Name: Hey You		
Aliases: Hey You	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 928	**See Also:**
Notes: This virus contains the following text: Hey, YOU !!! Something's happening to you ! Guess what it is ?! HA HA HA HA ...		

Name: HH&H		
Aliases: HH&H, GMB, Gomb	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 4091	**See Also:**
Notes: Contains the text "HARD HIT & HEAVY HATE the HUMANS !!".		

Name: Hi		
Aliases: Hi	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 460	**See Also:**
Notes: Contains the text "Hi" v6-151: At least one anti-virus program can detect and remove Hi.895		

Name: Hide and Seek		
Aliases: Hide and Seek	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 709	**See Also:**
Notes: The virus displays the message: Hi! boy. Do you know 'hide-and-seek' ? Let's play with me!!.		

Name: Hidenowt		
Aliases: Hidenowt	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-123: Hidenowt Disables Ctrl-Break checking v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Highlander		
Aliases: Highlander	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:** 477	**See Also:**
Notes:		

Name: Hitchcock		
Aliases: Hitchcock	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1247	**See Also:**
Notes: Plays a tune from the Hitchcock TV series		

Name: HLLC		
Aliases: HLLC, Even Beeper, Antiline	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove HLLC (Even Beeper.C and Even Beeper.D)		

Name: Horror		
Aliases: Horror	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.	**Features:** EncryptedDirect acting.	
Damage: Unknown, not analyzed yet.	**Size:** 111211371182	**See Also:**
Notes:		

Name: Horse		
Aliases: Horse, Naughty Hacker	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes: A family of 8 viruses		

Name: Horse Boot virus		
Aliases: Horse Boot virus	**Type:** Boot sector.	
Disk Location: Hard disk boot sectors.Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:** Horse virus
Notes: Same author as the Horse virus.		

Name: Horse II		
Aliases: Horse II, 1160, 512	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.Program overlay files.COMMAND.COM	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Overwrites sectors on the Hard Disk.	**Size:** 1160	**See Also:**
Notes: The Horse II virus is a 1160 byte memory resident, stealth virus. It infects .COM applications including command.com, .exe applications, and program overlay files. We don't kown what the damage mechanism is yet. Similar in name but not function to Horse Boot virus 9 variants of Horse viruses, sometimes identifies it as 512, which is wrong. Most found in some schools in Sofia.		

Name: Houston B1		
Aliases: Houston B1	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** StealthMemory resident; TSR.	
Damage: Unknown, not analyzed yet.	**Size:**	**See Also:**
Notes:		

Name: Hungarian		
Aliases: Hungarian, Hungarian-473	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Attempts to format the disk.	**Size:** 482473	**See Also:**
Notes: Activates on Nov 7 and formats the hard disk. The 473 variant activates on June 13.		

Name: Hydra		
Aliases: Hydra	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** 340-736	**See Also:**
Notes: A series of 8 viruses		

Name: Hymn		
Aliases: Hymn	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v5-101: The Murphy and Hymn viruses are considered to be from separate families, although they include sections of code from the Dark Avenger (Eddie) virus.		

Name: Icelandic		
Aliases: Icelandic, Disk Eating Virus, Disk Crunching Virus, One In Ten, Saratoga 2	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Corrupts the file linkages or the FAT.	**Size:** 656 -671 Length MOD 16 will always be 0.	**See Also:**
Notes: Infects every 10th .EXE file run, and if the current drive is a hard disk larger than10M bytes, the virus will select one cluster and mark it as bad in the first copy of the FAT. Diskettes and 10M byte disks are not affected. File length increases. Decreasing usable hard disk space. Infected .EXE files end in 18 44 19 5F (hex). System: Byte at 0:37F contains FF (hex)		

Name: Icelandic II		
Aliases: Icelandic II, One In Ten, System Virus, 642	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 632-647 Length MOD 16 will always be 0.	**See Also:**
Notes: Every tenth program run is checked, and if it is an uninfected .EXE file it will be infected. The virus modifies the MCBs in order to hide from detection. This virus is a version of the Icelandic-1 virus, modified so that it does not use INT 21 calls to DOS services. This is done to bypass monitoring programs. EXE Files: Infected files end in 18 44 19 5F (hex). System: Byte at 0:37F contains FF (hex)		

Name: Icelandic III		
Aliases: Icelandic III, December 24th	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 848 - 863	**See Also:**
Notes: It infects one out of every ten .EXE files run. If an infected file is run on December 24th it will stop any other program run later, displaying the message "Gledileg jol"		

Name: Infector		
Aliases: Infector	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Infector (759 and 822.B)		

Name: Int_10		
Aliases: Int_10	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:**	
Damage:	**Size:**	**See Also:** monkey

Notes: v6-143:
discovered in Canada late 1993. payload is a graphic snowfall on the screen at midnight or 6 hours following boot in December, could cause disk corruption.
"This virus goes resident in 1k at the TOM and actually removes itself from the fixed disk during boot replacing the original MBR into sector one to avoid detection. While it eventually hooks interrupt 13h, this is not during the BIOS load, being accomplished through DOS instead.

Once fully resident, "stealth" is used to hide the return of the virus to the MBR.

While two varients have been found so far, both may be detected via the following string in the MBR (if booted from floppy), a floppy DBR, or in the last 1k area at the TOM if resident in RAM;

88 85 93 02 41 41 D3 E0 80 7D 0B 00 75

At the moment this virus which has been tentatively named INT_10 has been observed at a single location only."

v6-146: Killmonk 3.0 is available via ftp at ftp.srv.ualberta.ca, in the file pub/dos/virus/killmnk3.zip. A small text manual, and technical notes on Monkey and Int_10 are included with the package. I'm not a mail server, but if you can't do ftp, but do know how to use uudecode, then I might find time to email KillMonk 3.0 to you, if you ask nicely. :) Written by Tim Martin, martin@ulysses.sis.ualberta.ca

Name: Intruder		
Aliases: Intruder	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Intruder.1317.		

Name: Invader		
Aliases: Invader, Plastic Boot	**Type:** Boot sector.	
Disk Location: COM application.EXE application.Hard disk boot sector.Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorCorrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A multipartite virus: infects both files and boot area once the virus has become installed in memory The V101 virus is a multipartite virus too.		

Name: Invol		
Aliases: Invol	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Involuntary		
Aliases: Involuntary	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Device Driver infector		

Name: INVOLVE		
Aliases: INVOLVE	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: maybe this virus doesn't exist - v5-193 changes the date on files it has infected.		

Name: Israeli Boot		
Aliases: Israeli Boot, Swap	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: It infects floppy disk boot sectors and reverses the order of letters typed creating typographical errors.		

Name: Italian Boy		
Aliases: Italian Boy	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: IVP		
Aliases: IVP, Bubbles, Math, Silo, Wild Thing, Mandela, Swank	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove IVP (540, Bubbles, Math, Silo and Wild Thing)		

Name: Jack the Ripper		
Aliases: Jack the Ripper, Jack Ripper	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.Stealth	
Damage: Corrupts a program or overlay files.Corrupts a data file.Corrupts floppy disk boot sectorCorrupts hard disk boot sector	**Size:**	**See Also:**
Notes: A boot sector virus, infects memory, boot, MBR. Don't scan for viruses with this virus in memory, it'll infect It is two sectors long, and has some minor encryption in it. The encryption is two strings and some executible code in the boot record . It wants to be stealthy, but it doesn't do anything significantly stealthy. Approximately once a minute there is a check to see if you are writing to the disk, if you are, it does minor garbling of a disk sector		

Name: Jackal		
Aliases: Jackal	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Japanese_Christmas		
Aliases: Japanese_Christmas	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Japanese_Christmas.600.E		

Name: Jeff		
Aliases: Jeff	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: non resident com infector		

Name: Jerusalem		
Aliases: Jerusalem, Jerusalem A, Black Hole, Blackbox, 1808, 1813, Israeli, Hebrew University, Black Friday, Friday 13th, PLO, Russian, Kylie (variant), Scott's Valley, Mule, Slow,Timor, Zerotime, Zerotime.Australian	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Deletes or moves files.	**Size:** 1813 Change in size of .COM files1808-1823 .EXE files: length mod 16 is 0Multiple infections of .EXE files are possible	**See Also:**
Notes: Spreads between executable files (.COM or .EXE). On Friday the 13th, it erases any file that is executed, and on other days a two line black rectangle will appear at the bottom of the screen. Once this virus installs itself (once an infected COM or EXE file is executed), any other COM or EXE file executed will become infected. Kylie is difficult to spread. Mule variant uses encryption. EXE files too large to run, odd screen behavior and general slowdown, works well on LANs 1. "MsDos" and "COMMAND.COM" in the Data area of the virus 2. "MsDos" are the last 5 bytes if the infected program is a .COM file.		

Name: Jerusalem-B		
Aliases: Jerusalem-B, Jerusalem-C, Jerusalem-D, Jerusalem-DC, Jerusalem-E, Jerusalem-E2, New Jerusalem, Payday, Skism-1, Anarkia, Anarkia-B, A-204, Arab Star, Mendoza, Park ESS, Puerto	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Direct acting.	
Damage:	**Size:** 1808	**See Also:**
Notes: Works well on LANs		

Name: Jest		
Aliases: Jest	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Jest.		

Name: Joe's Demise		
Aliases: Joe's Demise, Joes Demise	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program file.	**Size:** 1 Ka 10 byte COM file was increased to 1928 bytes	**See Also:**
Notes: file infector, infects both .COM and .EXE files. It does not seem to effect .SYS or overlay files. File size shows a 1K increase when infected but the time and date stamps do not change. Stealth technique used: It detaches itself from the infected files when they are run. Windows may not load We identified the following as a valid search string for the new virus; 5A 5B 07 1F C3 1E 52 2E		

Name: Joker		
Aliases: Joker, Jocker	**Type:** Program.	
Disk Location: EXE application.DBF files	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, length changes	**See Also:**
Notes: Joker is a non-resident .EXE infector. It may also infect .DBF files. It overwrites the attacked file with the virus code. It was discovered in Poland in 1989. It is a poor replicator, and is probably extinct. There are many strange strings at the beginning of the file that are printed on the screen. It may cause system hangs. Some of the strings are: "END OF WORKTIME. TURN SYSTEM OFF!", "Water detect in Co-processor.", "I am hungry! Insert HAMBURGER into drive A:" Strange messages. .EXE files change length. File length changes, strange messages delete files		

Name: JOKER-01		
Aliases: JOKER-01, Joker-01 Joker 01, Joker 2	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 29233 to 2937229233	**See Also:**
Notes: A resident .EXE and .COM infector. It does not infect COMMAND.COM. The infection is at the end of the file. .EXE files are converted to .COM file signatures with a small loader inserted at the beginning of the file. The display may clear and the system may hang with this virus in memory. Random letters may appear on the screen. The string "JOKER-01" is in the file. The infection method is similar to VACSINA. System hangs. Strange letters on screen. File lengths change. String "JOKER-01" found in file. Scan file for string "JOKER-01" Delete files		

Name: Joshi			
Aliases: Joshi, Happy Birthday Joshi, Yoshi?	**Type:** Boot sector.		
Disk Location: Hard disk boot sectors.Floppy disk boot sectors.		**Features:**	
Damage: Infects Master BooT record		**Size:**	**See Also:**

Notes: A new variant seems to be able to intercept BIOS calls.
Will infect a second physical hard drive if it is present. FDISK/MBR will only clean up the first physical hard drive.
on Jan 5 will ask you to type "happy birthday joshi" and only after you type it you can continue maybe came from India
Virus exists in the partition table on HD, on Floppies it resides in the boot sector and on an additionally formatted tract (number 40 or 80, depending on diskette size)

the next 3 paragraphs are from virus-l, v6-105:

"Before attempting any Joshi virus removal (or even detection!), you must make sure that there is no virus present in memory. For that purpose, you must COLD boot from an uninfected, write-protected system diskette. If you fail to do that, the virus can remain active in memory, and either stealth the fact that it is present on the disk, or re-infect the disk right after it has been disinfected, or both.

Note the word "cold" in the paragraph above. This means that you have to turn your computer off and then switch it on again - or press the Reset button, if your computer has one. Just pressing Alt-Ctrl-Del might not be sufficient with some viruses - and it isn't sufficient with Joshi.

The reason is that Joshi intercepts those keys and fakes a reboot, while in practice remaining active in memory. An experienced user will undoubtedly notice that on most kinds of computers (because the boot simulation is not perfect - it just cannot be), but many users will be fooled to believe that they have really rebooted their machine."

Name: Jumper		
Aliases: Jumper, French Boot, Sillybob, Neuville, Touche, EE, 2KB, Viresc, Jumper B	**Type:** Boot sector.	
Disk Location: Hard disk partition table.Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Display s message on boot-up.	**Size:** Recudes memory by 2 kbyte and uses that for itself.	**See Also:**

Notes: Jumper infects diskette boot sectors and hard disk MBRs .
It infects the hard disk only if the user tries to boot from an infected floppy.
Most, but not all floppies used in the computer are then infected.

The virus sometimes hangs the machine at boot.

This virus intercepts Int 21h and Int 1Ch. It uses Int 1Ch, which is the system Timer Tick , to activate its triggering routine. Every time the timer ticks, the virus compare the 2nd lowest byte of the timer in BDA area with offset 01C6h in boot sector. As soon as the value in timer exceeds the value at the boot sector, the virus hooks Int 21h. Two sub-functions of Int 21h are employed for infection drives A and B. The sub-function 0Eh will be used to infect drive A or B immediately. The sub-function 0Ah will be used along the clock time tests for infecting the drives A and B. Sometime, on booting, the virus locks the machine by repeatedly displaying 'e '. All these activities are closely tied to the clock count in BDA, since the count change 18 times in 1 second, the activities are sparse and almost random.

Removal of the virus should be done under clean system condition and using the FDISK/MBR command.

For more info., see the VIRUS BULLETIN April 1995 issue.

Name: JUNKIE		
Aliases: JUNKIE	**Type:** Multipartite.	
Disk Location: Floppy disk boot sector.Hard disk partition table.COM application.	**Features:** Encrypted	
Damage: Interferes with a running application.	**Size:** Overlays boot sector, no increase	**See Also:** Smeg

Notes: Junkie, reportedly first infected a company in the Netherlands after being downloaded from a bulletin board.
iJunkie is a multi-partite virus that infects hard drive MBR, floppy disk boot record and .COM files.
Junkie is not a stealth virus.
It is variably encrypted, but not polymorphic.
No "trigger" or "payload" have been identified for the Junkie virus.

NAV Will Detect & Repair Junkie Virus

Name: Justice		
Aliases: Justice	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: Once found in the wild in Bulgaria		

Name: K-4		
Aliases: K-4	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove K-4 (687 and 737).		

Name: Kamikazi		
Aliases: Kamikazi	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Rare virus. Overwrites the beginning of an infected file Damages the first four bytes of an infected file		

Name: Kamp		
Aliases: Kamp, Telecom 1, Telecom 2, Kamp-3700, Kamp-3784, Holo	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: KAOS4		
Aliases: KAOS4, Kaos 4, Sexotica	**Type:** Program.	
Disk Location: EXE application.COM application.COMMAND.COM	**Features:** Direct acting.Non stealthDesigned to avoid detection by heuristic scanners.	
Damage: Interferes with a running application.No damage, only replicates.	**Size:** 697	**See Also:** Vienna

Notes: The KAOS 4 virus is a variant of the Vienna virus that has been extended to infect .EXE files as well as .COM files. The virus is direct acting, and randomly infects one .COM and one .EXE file every time it is run. It attacks COMMAND.COM first. On my machine, it seemed to prefer the \DOS and the \NU (norton) directories. The virus adds 697 bytes to the length of both .COM and .EXE files, the modification date of the files does not change. The following text is in the clear in the last sector of an infected file: KAOS4 / Köhntark.
For *.COM files case, When the file is less than 64K and if it does not start with E9??h ??20h , then the target *.COM file will be infected.
It is not detected by DataPhysician Plus 4.0D or SCANV116. A virus signature file is available from DDI named KAOS4.PRG that works with version 4.0C. There is a problem with using it with version 4.0D. load it into Virhunt by using the Options - E (user signature file) command and type the file name, or load it at startup with VIRHUNT USC:\DDI\KAOS4.PRG (assuming that kaos4.prg is in your DDI directory on your C drive. Then run a normal scan. Virhunt will identify it as an "Unknown Virus". Virhunt can also apparently remove this virus from files using this virus signature file.
The virus does not seem to have a payload, though while not intentionally damaging, infected systems become unbootable.
The next version of SCANV is also supposed to detect the virus (probably 117).
The virus is not detected by ThunderBYTE.

Name: Kemerovo		
Aliases: Kemerovo	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Kemerovo.257.E.		

Name: Kennedy		
Aliases: Kennedy, 333, Dead Kennedy, Danish Tiny, Stigmata, Brenda	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts the file linkages or the FAT.	**Size:** 3331631000 (Stigmata Variant)256 (Brenda Variant)	**See Also:**

Notes: When an infected file is run, it infects a single .COM file in the current directory. On June 6th, November18th and November 22nd it displays the message:

Kennedy er d¢d - længe leve "The Dead Kennedys"

The Brenda variant contains the text:

(C) '92, Stingray/VIPER
Luv, Brenda

v6-151: At least one anti-virus program can detect and remove Danish Tiny (163 and Kennedy.B)

Name: Kernel		
Aliases: Kernel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: v6-151: At least one anti-virus program can detect and remove this virus.

Name: Keypress		
Aliases: Keypress	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1232-1247 in .COM file.1472-1487 in .EXE file.	**See Also:**

Notes: Every 10 minutes, the virus looks at INT 09h (keyboard interrupt) for 2 seconds; if a keystroke is recognized during this time, it is repeated depending on how long the key is pressed; it thus appears as a "bouncing key"
v6-140: At the moment I know of the following variants:

1215	1215/1455 bytes
1228	1228/1468 bytes
9 variants of 1232	1232/1472 bytes
1236 (Chaos)	1236/1492 bytes
1266	1266/1506 bytes
1495	1495/1735 bytes
1744	1744/1984 bytes
2728	2728/2984 bytes

A total of 16 variants...whatever CPAV identifies as "KEYPRESS 5" is probably one of them, but without information on the virus size I cannot tell which one it is. -- frisk

v6-141: " ...I have just tested CPAV 2.0 on my collection of Keypress variants, and the one that it calls KeyPress 5 is something that we call Keypress.Ufo... "
v6-142: "...CPAV 2.0 calls "KeyPress 5" only the last one - Keypress (2728) in your naming scheme...."

Name: Knight		
Aliases: Knight	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name:KOH		
Aliases: KOH, StealthBoot-D, King of Hearts, Potassium Hydroxide	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**

Notes: It basically encrypts disks for the user using a user-defined password - asking permission before infecting hard drives (and recommending a backup) and allowing a toggle-key for floppy infection, as well as one for uninstallation from the hard-drive (complete decryption, removal of interrupt handlers, and replacement of the old Master Boot Record).

The KOH virus comes in it's initial installation package as a 32000 byte COM. It is a comparitively "user-friendly" virus, with un-installation routines and a floppy-infection toggle. It's purpose is this: when run, it asks for a password - it will encrypt the floppy using this password and the IDEA encryption algorithm (not yet verified by my disassembly). When the floppy is rebooted from, it will ask for permission to infect the hard drive, and recommend a backup beforehand. It will then ask for a password for the Hard-Drive to be encrypted with, and ask whether to use IDEA encryption or a simple routine

After the encryptions have been installed: the virus will ask for passwords on bootup for the Hard-drive and floppy - this will be used to encrypt/decrypt calls that would read or write to the disk. The floppy password may be changed at any time, allowing the reading of any encrypted floppy as long as the user knows the password. The function-keys for the virus are as follows:

CTRL-ALT-K Set new floppy password
CTRL-ALT-O Toggle Floppy Infect
CTRL-ALT-H Uninstall Virus From Hard-Drive

Notice that there is no floppy uninstall...

Name: Lapse		
Aliases: Lapse	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Lapse (323, 366, and 375)		

Name: Leapfrog		
Aliases: Leapfrog, 516	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**

Notes: Does not change the file entry point. (other viruses that are similar are Voronezh-1600 and Brainy)

Leapfrog modifies the instruction the initial JMP points to (for COM files)
v6-084: will not be noticed by the integrity checking of MSAV (DOS 6.0 antivirus)

Name: Lehigh		
Aliases: Lehigh, Lehigh-2, Lehigh-B	**Type:** Program.	
Disk Location: COMMAND.COM	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Corrupts the file linkages or the FAT.Corrupts boot sector	**Size:** Overlays application, no increase555 bytes inserted in stack area of COMMAND.COM.	**See Also:**
Notes: Spreads between copies of COMMAND.COM. After spreading four or ten times, it overwrites critical parts of a disk with random data. Displaying junk on the screen. Alters the contents and the date of COMMAND.COM. Spread will be detected by any good modification detector.		

Name: Leningrad		
Aliases: Leningrad	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A friday the 13th time bomb virus that may or may not format the disk v6-151: At least one anti-virus program can detect and remove Leningrad II.		

Name: Leprosy		
Aliases: Leprosy, Leprosy 1.00, Leprosy-B, News Flash, Clinton	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 350647	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Liberty		
Aliases: Liberty, Liberty-B, Liberty-C	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Corrupts boot sector	**Size:** 2862 bytes	**See Also:**
Notes: Self-encrypting, not known if destructive floppy boot infection occurs rather rarely and is possible on PC XTs only Scanners don't seem to report an infection when tested against an infected floppy. INT 1CH is used to trigger. When triggered, the virus changes all characters being sent/received via INT 14H, printer via INT 17H and displayed via INT 10H (AH=09 or AH=0AH) toomake a string "MAGIC!!" for 512 timer ticks (approx 28 secs). After 10th triggering the virus swaps the upper line of a screen for blinking yellow-on-red sign "M A G I C ! ! !" (won't work on monochromes) then passes cotrol to ROM Basic. PCs without ROM Basic will either hang or reboot. On self-encrypting: only self-encryps small piece of code used to infect COM files. Also encrypts first 120 bytes of infected COM file but this is NOT SELF-encrypting		

Name: Lisbon		
Aliases: Lisbon, Vienna, Vienna 656, VHP related (?)	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 648 bytes added to the end of the file.	**See Also:**
Notes: Vienna Virus strain. The time stamp of an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the file size<10 or file size>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 58h) <> 0 ELSE damaged! A selected .COM-file is damaged permanently by overwriting the first five bytes by "@AIDS" Damaged applications Easy identification.: Last five bytes of file = "@AIDS" (Ascii) The time stamp of an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). Replace damaged files.		

Name: Literak		
Aliases: Literak	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Little Girl		
Aliases: Little Girl	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Little Girl.985.		

Name: Little Red		
Aliases: Little Red, Little.Red, Mao	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.Semi-Stealth Infecting process results in slowing down the computer	
Damage: Audio messages under certain conditions.	**Size:** 1465 bytes long.	**See Also:**

Notes: The following are extracted from the VB, July 1995:

The Little.Red virus is written to commemorate the Chinese leader " Mao-Tse Tung ". It deliver its payload on Sep. 9 and Dec. 26 on any year larger 1994. On Dec. 26 (Mao's birthday), It plays the Chinese tune ' Liu Yang River ' , this river runs through the Hunan province or Mao's birthplace. On Sept. 9 (the death date of Mao-Tse Tung), it plays the Chinese tune 'The East is Red'.
The virus body is appended to the COM and EXE files and the file beginning is modified according to file type. Both infected EXE and COM are capable of infecting the memory and they are functionally the same. However, the memory resident copy resides in different location in memory.
Little.Red's ID in memory is the BL register returns a value of 5Bh. In EXE file, the Initial IP is equal to 693. In COM file, the first byte is JMP, then a mathematical operation is performed on 2nd and 3rd byte, if the result equals to the contents of 4th and 5th byte, then the COM file is infected.

The installation method in memory is done in the usual way. Suppose an infected COM file is executed, control is passed to the virus code which checks for its ID in memory. If no resident copy is found, then it decrypts the code, executes installation routines, re-encrypts the code and returns control to the host file. The installation routine use DOS call Int 21h, function 4Ah (Resize Memory Block) to shrink memory by 6Dh paragraphs and copy itself into that space at the end of the memory block. The last part of the procedure is to hook Int 21h, Int 1Ch, and attempt to infect COMMAND.COM file(not successful). The resident copy of the virus hooks several subfunctions of Int 21h for its use, they are:
AH = 11h , AH = 12h, AH = 30h, and AX = 4B00h.

The virus is rather eager to infect as many files as possible when DIR command is issued, however, the draw back is that the machine becomes very slow when there many clean EXE and COM file in the directory. This sluggishness is also accompanied by disk clanking and it gives a clue to the presence of the virus.

As it was mentioned above, Little.Red does not carry any destructive payload. However, the continuous music could be irritating and nerve racking to some people.

The recommended method for disinfection is to use clean system conditions, then identify and replace the infected files.

Name: Lock-up		
Aliases: Lock-up	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Loki		
Aliases: Loki	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Loki.1234.		

Name: Loren		
Aliases: Loren	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.	**Size:**	**See Also:**
Notes: v6-125: Loren infects all .COM and .EXE files opened for execution and all files referenced by Int 21 fn 11 and 12, which are obsolete commands still used by the DIR command. Thus, if the virus is in memory, using DIR will infect all COM and .EXE files opened. The virus hides increases in file length when active in memory. The virus counts the number of files infected, and if the counter reaches 20 the warhead is triggered. This tries to format cylinder 0, head 0 on drive C. If this fails, it tries drives A and B. If it suceeds in formatting any drive the following message is put to screen: Your disk is formatted by the LOREN virus. Written by Nguyen Huu Giap. Le Hong Phong School *** 8-3-1992 and the counter is reset. A low level format will usually be needed to recover affected hard disks.		

Name: Lyceum		
Aliases: Lyceum	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Lyceum.930.		

Name:LZ		
Aliases: LZ	**Type:** A Companion virus	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This companion virus makes a copy of itself with .com extension, and duplicates the name of all .exe files so it gets run first. Non-resident virus. Looks in current directory for an exe file. makes com file with same name, finds one at a time. Only one version (scan 86) finds it, it had too many false alarms so they took it out. LZ is a valid compression utility, that was causing lots of false alarms. Look in directory, see .com file there that has same name. (com file may be hidden) This one was tough to find, McAfee version should NOT be detecting it (too many false alarms)		

Name:LZR		
Aliases: LZR, GenBP, Gen B, Stoned.LZR	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR above TOM.Stealth	
Damage: Corrupts a program or overlay files.	**Size:** Reduces real memory by 1K	**See Also:**
Notes: Because of the stealth, It is difficult to detect or remove. When the vvirus is not resident, an infected sector contains the letter r followed by a two character variable counter at offset 114.		

Name: M_jmp		
Aliases: M_jmp	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove M_jmp (122, 126, and 128)		

Name: MacGyver		
Aliases: MacGyver, McGyver, Shoo, Mad Satan, Satan, Mcgy	**Type:** Program.	
Disk Location: COM application.EXE application.Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.Stealth	
Damage: Unknown, not analyzed yet.	**Size:** 2803282431604112 4480, 4645	**See Also:**

Notes: MacGyver is a family of viruses with different properties and text.

Variant:Properties:Text
MacGyver.2803 : Infects EXE files: MACGYVER V1.0 Written by JOEY in Keelung. TAIWAN
MacGyver.2824A : Infects EXE files : MACGYVER V1.0 Written by JOEY in Keelung. TAIWAN
MacGyver.2824B : Infects EXE files : * Satan Virus * MAD !! Another Masterpiece of Sax (c) Copyright 1993 Written by Mad Satan... Ver 2.02
MACGYVER V1.0 Written by JOEY in Keelung. TAIWAN
MacGyver v4.0 written by Dark Slayer in Keelung,
Taiwan. 93/09/09
MacGyver.3160 : Infects COM and EXE files
MacGyver.4112 : Infects COM and EXE files and boot sectors
MacGyver.4480 : Infects COM and EXE files, stealth: MacGyver v4.0 written by Dark Slayer Taiwan. 93/09/09
MacGyver.4643 : Infects COM and EXE files
MacGyver.4645 : Infects COM and EXE files, stealth

F-Prot 2.19 detects this virus.
SCAN 226 detects variant 2824 as 2803 and incorrectly disinfects the files. Disinfected files become unusable. Scan removes the virus but does not fix the pointer to the start of the .EXE program so the first step jumps to where the virus used to be causing a crash or worse.

Name: Macho		
Aliases: Macho, MachoSoft, 3555, 3551	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Corrupts a data file.	**Size:** 3550-3560 bytes are appended on a paragraph boundary	**See Also:**

Notes: Spreads between .COM and .EXE files. It scans through data on the hard disk, changing the string "Microsoft" (in any mixture of upper and lower case) to "MACHOSOFT". If the environment variable "VIRUS=OFF" is set, the virus will not infect. Use this as a temporary protection. Microsoft changes to MACHOSOFT Search for the string: 50,51,56,BE,59,00,B9,26,08,90,D1,E9,8A,E1,8A,C1,33,06,14,00,31,04,46,46,E2,F2,5E,59

Name: Magician		
Aliases: Magician	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Maltese Amoeba		
Aliases: Maltese Amoeba, Irish, Grain of Sand	**Type:** Program.Memory resident - TSR	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Overwrites MBR/prints msg on 11/1 & 3/15	**Size:** Variable, dur to variable length of encryption headerPolymorphic: each infection different	**See Also:**
Notes: widespread in Ireland& UK, a dangerous polymorphic multi-partite fast infector (virus-l, v5-006) On Nov 1 or March 15 it replaces MBR of hard drive and displays a message that says something like "Amoeba virus by Hacker Twins...Just wait for Amoeba 2". The message refers to he University of Malta. This virus was probably very aware (or wrote) the Casino virus, as when it initially infects, it checks for the existance of the Casino, and if its there, it takes over INT 21 from it (thereby eradicating Casino) and places itself there instead. Signature scans don't work for this virus, an algorithmic check is the best way to locate it. No strange activity until activation date, at which point much text gets printed to the screen and the computer hangs. Not many anti-viral programs as of March 6, 1992. Data Physician Plus! v3.0D Note: PKZIP 2.04C causes false positives for this virus, especially with CPAV, or the microsoft version of CPAV.		

Name: Manuel		
Aliases: Manuel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Manuel (777, 814, 840, 858, 876, 937, 995, 1155 and 1388)		

Name: MAP		
Aliases: MAP, FAT EATER	**Type:** Trojan.	
Disk Location: MAP.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This is another trojan horse written by the infamous "Dorn Stickel." Designed to display what TSR's are in memory and works on FAT and BOOT sector. FAT EATER		

Name: Marauder		
Aliases: Marauder	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Markt		
Aliases: Markt	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Trashes the hard disk.on Sept. 9	**Size:**	**See Also:** vcl

Notes: Washington Post Business Section

> >"A computer hacker with the nickname 'The Wizard' has distributed a virus
> >that is set to destroy
> >data on thousands of computers next month, German retail group Media Markt
> >said. The virus
> >could affect more than 10,000 personal computers worldwide."

Well yes the virus exists its name is Markt. on the 9.th of September
it will write garbage (1990 sectors through INT26) to every logical and local
partition it can find beginning with C: and ending with Z:
It is a simple, lightly encrypted virus based on the VCL (virus construction
lab), but manually 'enhanced'. It also displays a skull, a Media Markt logo, and
a stupid message on the trigger date.
It was only sighted in southern Germany, Switzerland and Austria.....
NO NEED FOR PANIC ESPECIALLY IN THE US!!!!!

> >It is possible that the "Markt" name could be a Post typo, but I am
> >unsure. Perhaps y'all could investigate and let us
> >know what our vulnerability might be and what packages might detect it.
> >At least, with this notice, we have some
> >planning time if it is a real virus alert.
Current AV products like McAfee SCAN, F-PROT, and TOOLKIT detect and eradicate
the virus...

Name: MATHKIDS		
Aliases: MATHKIDS, FIXIT	**Type:** Trojan.	
Disk Location: FIXIT.ARC	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**

Notes: This trojan is designed to crack a BBS system. It will attemp to copy the USERS file on a BBS to a file innocently called FIXIT.ARC, which the originator can later call in and download. Believed to be designed for PCBoard BBS's.

Name: Matura		
Aliases: Matura	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: v6-151: At least one anti-virus program can detect and remove Matura.1626

Name: Mel		
Aliases: Mel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: v6-151: At least one anti-virus program can detect and remove this virus.

Name: Merritt		
Aliases: Merritt, Alameda, Yale, Golden Gate, 500 Virus, Mazatlan, Peking, Seoul, SF Virus	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorCorrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Track 39 sector 8 is used to save the original boot record, and any file there will be overwritten. Destroys the FAT after some length of time. It spreads when the Ctrl-Alt-Del sequence is used with an uninfected diskette in the boot drive. The Golden Gate variation will reformat drive C: after n infections. Infects Floppies Only. Spreads between floppy disks. Unbootable disks, destroyed files. 80286 systems crash. Compare boot sector of infected disk with a "real" system disk. If different: check track 39, sector 8; if this contains the real boot blocks. Execute a SYS command to reinstall real boot block and system file from a clean disk.		

Name: Merry Christmas		
Aliases: Merry Christmas	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Mexican Stoned		
Aliases: Mexican Stoned, stoned variant	**Type:** Memory resident; TSR.Activates once at boot time.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Prints out "No votes por el pri" which is spanish for "Don't vote for el Pri" (a political party)		

Name: MGTU		
Aliases: MGTU	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Mgtu (269, 273.B and 273.C)		

Name: Michelangelo		
Aliases: Michelangelo, Michaelangelo, Mich	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.Hard disk partition tables.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increaseMoves orig. boot sector elsewhereUses Interrupts INT 13 and INT 1A	**See Also:**

Notes: First identified in the summer of 1991. This virus is similar to the Stoned, but utilizing some different techniques, so it's not simply a Stoned variant. It works for any version of MS DOS.
Triggers: Bootup from an infected disk will infect. Usage of floppy a: drive (read, write, or format) will cause infection of that medium. Payload: on March 6 (Michaelangelo's birthday) this virus will destroy data by overwriting the medium the computer was booted from. Hard disks will have sectors 1-17 on heads 0-3 of all tracks, floppies: sectors 1-9 or 1-14 on both heads and all tracks depending on the FAT type will be overwritten.

When Stoned and Michaelangelo both infect a disk, problems occur because they both try to hide the partition table in the same place. March 6th (Michaelangelo's birthday) data destruction.

Upon bootup from an infected floppy the virus will go memory resident and infect the partition table. Any INT13 is intercepted thereafter. Any floppy A: operation will infect the disk in drive A: provided the motor was off (this cuts excessive infection testing).

When the virus is resident, CHKDSK will return a "total bytes memory" value 2048 less than normal. for a 640k PC normal=655,360; with virus: 653,312

Most anti-viral untilities will detect and remove it. Also, boot from a clean disk and move the original sector to its proper location (sector 1 head 0 track 0); on some systems FAT copy 1 might be damaged, so an additional copy of FAT 2 ont FAT 1 might be necessary

Name: Milan		
Aliases: Milan, Milan.WWT.67.C	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Milena		
Aliases: Milena	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** increases by 1160	**See Also:**

Notes: Installs itself using standard Mem Alloc (DOS service 48) and INT 21 will be hooked by it. After becoming resident, and EXE or COM opened to create, open, chmod, load&exec, rename, or new file will be infected

Opened TXT files will be overwritten at the end with the string "I Love Milena...". Infected files contain strings "LOVE" and "I Love Milena"
A search string is 3D 21 25 74 0E 3D 21 35 74 15

Name: minimal		
Aliases: minimal, minimal-45, 45	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 45 bytes!	**See Also:**
Notes: World's smallest virus. Only 45 bytes long. Non-resident program infoctor. No known damage. users of F-PROT can add the following line to SIGN.TXT to detect it. Minimal-45 dOT5v5ememVLstmMnMLdjSmmWtMpGfnBv2w7U7GFTBWdhvtgjLErsbwR71YJI1xfLd		

Name: Minimite		
Aliases: Minimite	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Mirror		
Aliases: Mirror, Flip Clone	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 925933	**See Also:**
Notes: When the virus is triggered, the screen will flip horizontally character for character.		

Name: Mix1		
Aliases: Mix1, MIX1, MIX/1, Mixer1	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1618-1634 length mod 16 equals 0	**See Also:**
Notes: The output is garbled on parallel and serial connections, after 6th level of infection booting the computer will crash the system (a bug), num-lock is constantly on, a ball will start bouncing on the screen. Garbled data from the serial or parallel ports. Bouncing ball on the screen. "MIX1" are the last 4 bytes of the infected file.		

Name: Moctzuma		
Aliases: Moctzuma, Moctzuma-B	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Modem virus of 1989		
Aliases: Modem virus of 1989	**Type:** NONE, does not exist	
Disk Location:	**Features:**	
Damage: This virus is a myth!	**Size:**	**See Also:**
Notes: In December of 1989 there was a 'scare' about a modem virus being transmitted via a "sub-carrier" on 2400 bps modems. This is totally untrue, although reports of this mythical virus still occasionally occur. This information provided here to ensure that the myth goes no further.		

Name: Monkey		
Aliases: Monkey, Mon	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Stealth; actively hides from detection.	
Damage: Corrupts floppy disk boot sectorCorrupts hard disk boot sectorCorrupts boot sector	**Size:**	**See Also:** Int_10, Mon, Stoned.Empire.Monkey
Notes: Hides original partition table on cylinder 0, head 0, sector 3, and XOR's it with hex 2E (a "." character) SYS won't write a clean boot sector with Monkey, since it's a MBR infector. SYS works with floppies only Usually, most MBR viruses are removed with FDISK /MBR (dos 5.0 or up) but that doesn't work with Monkey because the Partition Table info in the MBR is not preserved. Program available (Nov 5, 1993) KillMonk v3.0 finds and removes the Monkey and Int_10 viruses. via ftp at ftp.srv.ualberta.ca, in the file pub/dos/virus/killmnk3.zip. The program claims it can also fix drives where the user has tried to use fdisk/mbr first. It's a very small virus, one sector, memory resident, MBR/stealth virus. it: 1. Tries to hide the virus infection - if you go to read the MBR, it redirects your inquiry and shows you the real MBR, not the virused one 2. Virus saves boot record, but masks it with character "2E" (which looks like a dot) and XOR's it, so to remove the virus you must un XOR (unmask) the real MBR. First version of Data Physician Plus! to find it is 3.1C 12/13/93: Karyn received one unconfirmed report that Data Physician Plus! 4.0B did not locate one variant of Monkey. v6-146: Killmonk 3.0 is available via ftp at ftp.srv.ualberta.ca, in the file pub/dos/virus/killmnk3.zip. A small text manual, and technical notes on Monkey and Int_10 are included with the package. I'm not a mail server, but if you can't do ftp, but do know how to use uudecode, then I might find time to email KillMonk 3.0 to you, if you ask nicely. :) Written by Tim Martin, martin@ulysses.sis.ualberta.ca		

Name: Monxla A		
Aliases: Monxla A, Monxla B, Time Virus, Vienna variant, VHP	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: A virus with a time bomb: on the 13th of any month it damages the files it tries to infect on that day only. It is a Vienna variant, it infects only files in the current directory and in the directories inthe path variable. Also can be identified as Vienna [VHP] virus		

Name: Moose		
Aliases: Moose, Moose31, Moose32	**Type:** Program.	
Disk Location: EXE application.COM application.COMMAND.COM	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 464-1700+ bytes	**See Also:**
Notes: One report of this virus in virus-l, v6-113, may be related to games, may not even be a virus.		

Name: MPS-OPC II		
Aliases: MPS-OPC II	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Mr. G		
Aliases: Mr. G	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Mshark		
Aliases: Mshark	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Multi		
Aliases: Multi	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Mummy		
Aliases: Mummy	**Type:**	
Disk Location: EXE application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Infects .exe files only		

Name: Murphy HIV		
Aliases: Murphy HIV, AmiLia, Murphy variant	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** Overlays application, no increase	**See Also:**

Notes: FPROT 2.01 identifies it as Murphy HIV.
A "fast file infector", it infects every file that is opened. No bounds have been found on the size of programs infected.

The text string "AmiLia I Viri - [NukE] i99i" appears at the beginning of the infection. The text section also refers to "Released Dec91 Montreal". This indicates that the virus has spread extensively since its release. In vancouver, it appears toave been obtained in one instance from a BBS known as Abyss. Other indications that it has spread.

Name: Murphy-1		
Aliases: Murphy-1, Murphy, V1277, April 15, Swami, Exterminator, Demon, Goblin, Patricia, Smack, Stupid Jack, Crackpot-272, Crackpot-1951, Woodstock	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1277	**See Also:**

Notes: Murphy is a program virus that appends itself to any COM or EXE file larger than 1277 bytes. COM files must be smaller than 64226 bytes, however if a COM file larger than 64003 is infected, it will not run.
The virus also locates the original INT 13 handler and unhooks any other routines that have been hooked onto this interrupt and restores the interrupt to the original handler.
It infects files on execution and opening.
Between 10 and 11 AM, the speaker is turned on and off which produces a clicking noise.
See Summary below for comments on some of the abovementioned aliases Between 10 and 11 AM, the speaker is turned on and off which produces a clicking noise. The virus contains the string: "Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory."
v6-151: At least one anti-virus program can detect and remove Murphy 1277.B and Woodstock)

Name: Murphy-2		
Aliases: Murphy-2, Murphy, V1521	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:** 1521	**See Also:**

Notes: A variant of Murphy-1, Murphy-2 is a program virus that appends itself to any COM or EXE file larger than 1521 bytes. COM files must be smaller than 63982 bytes.
The virus also locates the original INT 13 handler and unhooks any other routinesthat have been hooked onto this interruptand restores the interrupt to the original handler.
Files are infected on execution and opening.
Between 10 and 11 AM a ball (character 07) bounces over the screen. Between 10 and 11 AM a ball (character 07) bounces over the screen. The virus contains the string: "It's me - Murphy. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory."

Name: Mutation Engine		
Aliases: Mutation Engine, Dark Avenger's Latest, Pogue, MtE, Sara, Sarah, Dedicated, Fear, Cryptlab, Groove, Questo, CoffeeShop, DAME (Dark Avenger Mutation Engine)	**Type:** Program.Virus Authoring Package	
Disk Location: COM application.	**Features:** EncryptedDirect acting.Polymorphic	
Damage: Corrupts a program or overlay files.	**Size:** could be any sizePolymorphic: each infection different	**See Also:**
Notes: The MtE is a mutatuon engine that makes an existing virus difficult to detect by changing a virus with each infection. The first is the demo virus in the package (a silly, non-resident, COM file infector, infects only the files in the current directory) and a virus, called Pogue, wihch has been available on some VX BBSes in the USA. See notes below about the mutating engine. 11/2/92 virus-l, v5-186: announcement of MtE test reports, can be found via anonymous ftp from ftp.informatik.uni-hamburg.de:pub/virus/texts/tests/mtetests.zip and cert.org:pub/virus-l/docs/mtetests.zip none yet, but anti-virus researchers have it and are working hard -2/14/92 v6-126: CoffeeShop has same author as Cruncher virus. v6-151: At least one anti-virus program can detect and remove Coffeeshop.1568.		

Name: Mutator		
Aliases: Mutator	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Mutator (307 and 459).		

Name: N8FALL		
Aliases: N8FALL	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM	**Features:** Memory resident; TSR.Stealth	
Damage: Sometime displays message.May drop a 'CHILD' non-polymorphic companion virus.May cause software problems (false free memory available) .	**Size:** About 5800 byte long.Polymorphic: each infection different	**See Also:**

Notes:
The following notes are extracted from VB, May 1995:
N8FALL is about 5800 byte long; It is quite complex and stealth, and employs DOS commands and functionality to its own advantage.

When an infected file is executed, the virus checks for itself in memory by finding the value at 000:05E0h. If the returned value is JMP VIRUS instruction, then N8FALL follows the instruction and determines that its indeed a memory resident. If the virus is memory resident, control is returned to the host program. Otherwise, It attempts to install itself in system memory.
First, N8FALL calls Int 13h, Int 21h, and Int 2Ah vectors to check to anti-virus program as well as using them for its own installation, infection, etc. If any found, then they are disabled for salve preservation. Second, It looks for HIMEM.SYS. It uses Int 21h handler to determine the residence of DOS interrupt handler. If interrupt handler is in high-memory, then the area next to it will be over written with JMP VIRUS instruction. If interrupt handler is in low-memory, then it will be overwritten with JMP VIRUS instruction. Next, it opens COMMAND.COM files and closes the file, now COMMAND.COM is infected. Finally, N8FALL decrypts the string 'C:\NCDTREE\NAVINFO.DAT' which is name used by Norton Anti-Virus program. Control now is returned to the host program.
The virus infects COM and EXE files. Before infecting any file, it conducts checks so that 1) anti-virus program are exclude. 2) floppy disk are not write-protected. 3) DOS error messages, VSAFE, and Microsoft's TSR are disabled. When all these conditions are satisfied, the virus examines the lower five bits of the file, if they are all set to 1, then it becomes a candidate for infection. Next, the last 24 bytes are read and decoded. The virus look for its ID in this area. If the file is already infected, then control is given to a routine that runs the virus. If the file is clean, then it appends itself at end of the file and the beginning will be modified according to file type. For EXE file, the IP field are modified to point to the virus. In COM files, JMP VIRUS instruction will written into first 3 bytes.

Sometime, N8FALL instead of infecting an EXE file, it drops a companion virus which is 527 byte long, then it prints the following message:

Any means necessary for survival
N8FALL/2XS
By the perception of illusion we experience reality
Art & Strategy by Neurobasher 1994 - Germany
I don't think that the real violence has even started yet

Then, it waits for a key to press and it continues.
The companion is fully function and completely independent of the ' parent'. It identified itself in memory (memory word at 0000:052D2 has a value of 5832h). Then, Int 21h performs checks to avoid derives A: or B: and F-PORT.EXE. Later, it creates a matching COM file to which it writes itself setting the date/time to 11:55:00, 01 January 1994. In addition, the COM file has the attributes of System/Hidden/Read-only. No other attempts are being make to hide its presence.

The recommended method for disinfection is to use clean system conditions, then identify and replace the infected files.

Name: Natas		
Aliases: Natas	**Type:** Multipartite.	
Disk Location: Floppy disk boot sector.Hard disk partition table.EXE application.COM application.	**Features:** Memory resident; TSR.StealthPolymorphic	
Damage: No damage, only replicates.	**Size:** 4744 for file infectionsOverlays boot sector, no increaseVariants as 4744, 4746, 4774,4988 bytes are known	**See Also:** Satan Bug

Notes: WildList TechNotes: The Natas Virus

The Natas virus infects program files, the DOS boot sector on floppies and the master boot record (MBR) on the first physical hard disk (drive 80h, the C: drive). It is a polymorphic, multipartite, stealth virus.

The virus code is two sectors in length and it reserves 6k of memory by modifying the available-memory word at 40:13. Thus, on a 640k machine, mem would report 634k and chkdsk would report 649216 bytes of free memory. Examining memory with debug, the two bytes at 0040:0013 would be 7A 02, and the virus's name "Natas" would be visible in memory at 9F9D:0003.

The virus body is stored, unencrypted, on 9 sectors near the end of track 0, head 0, on the hard drive. The virus stealths the infected MBR if it is in memory, but not these extended sectors. The virus name "Natas" can be seen near the end of the last virus sector using a disk editor.

Infected files grow by 4744 bytes, but the change in size is stealthed if the virus is in memory. The name "Natas" is in the encrypted portion of the virus body and is thus not visible. The virus's decryptor is extremely polymorphic.

The virus contains no intentionally damaging routines and does not affect data files. The virus appears to be incompatible with some memory managers. Problems have been reported when QEMM386 and DOS EMM386 become infected.

The virus was evidently programmed by Little Loc, the programmer of the Sat_Bug (Satan Bug, or Satan) virus. The Natas virus has been distributed as commented source code. It is widely reported in Mexico and has appeared in Los Angeles, New York, and Virginia.

WildList TechNotes - (C) 1994 by Joe Wells (CARO) - jwells@symantec.com
---

According to Microsoft, NATAS is often the cause of "Driver Error 01" from EMM386.

Additional notes from VB Dec. 1994:
The virus is triggered when it detects the debugger or on the (1/512) chance of loading from and infected disk. The trigger routine formats the entire hard disk.
The 4744 byte contains two text strings: " Natas " and " BLACK MODEM ". The 4774 byte contains the string " Time has come to pay (c) 1994 NEVER- 1". The 4988 byte contains the string the following string:
" Yes I know my enemies.
They're the teachers who taught me to me compromise, conformity, assimilation, submission, ignorance, hypocrisy, the elite all of whitch are American dreams (c) 1994 by Never-1 (Belgium Most Hates) Sandrine B. ".

Name: Naught		
Aliases: Naught	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 712865	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Net Crasher		
Aliases: Net Crasher	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:** Vienna
Notes:		

Name: Neuroquila		
Aliases: Neuroquila, Neuro.Havoc, Havoc, Wedding	**Type:** Multipartite.	
Disk Location: Floppy disk boot sector.EXE application.Hard disk partition table.	**Features:** StealthMemory resident; TSR above TOM.PolymorphicEncrypted	
Damage: Corrupts hard disk partition table	**Size:** 4644-4675	**See Also:** Tremor

Notes: The Neuroquila virus infects EXE files, MBRs on harddisks and boot sectors on floppies. The original MBR is encrypted.
The infected MBR does not contain a valid partition table, so removal of the virus from memory makes the hard drive unmountable. On Floppy disks, the virus formats an extra track to store the virus code.

The virus attempts to load into the UMB. If no space is available, it loads into the STACKS area.

The stealth capability hides all changes to the disk or filew while the virus is in memory.

Neuroquila is a retrovirus, and attacks VIRSTOP.EXE, DOSDATA.SYS, TBDRIVER, TBDISK, VSAFE, and TBUTIL

After several months, the virus displays the following text:

<HAVOC> by Neurobasher'93/Germany -GRIPPED-BY-FEAR-UNTIL-DEATH-US-DO-PART

Name: Never Mind		
Aliases: Never Mind	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: New York Boot		
Aliases: New York Boot, NYB, B1, stoned.1	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** StealthMemory resident; TSR.	
Damage: No damage, only replicates.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Unremarkable boot sector virus, except that it resides in memory and is stealth, so if it is in memory and you look at the boot sector you wouldn't see it. It has no trigger, and does nothing except replicate. It carries no obvious payload. The virus can be detected easily. Its is marked by 1 Kbyte loss of memory after booting. To remove the virus, boot from a clean system floppy disk. For hard disk, Under DOS 3.3 or later , use FDISK/MBR command. For older version of DOS, restore MBR from your backup, or move the continent of track 0, sector 11, head 0 to track 0,sector 1, head 0 (i.e. reverse the action of the virus). For floppy disk, use FORMAT/S command to remove the virus.		

Name: Nice Day		
Aliases: Nice Day	**Type:** Boot sector.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Nina		
Aliases: Nina	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Nina (B and C)		

Name: NMAN		
Aliases: NMAN, NMAN B, NMAN C, C virus, Nowhere Man	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Direct acting.Not memory resident	
Damage: Corrupts a program or overlay files.Attempts to format the disk.	**Size:**	**See Also:**
Notes: Can get false positives because this virus was written in C and you might get the compiler to hit. Not memory resident, this virus is non-removable because it overwrites part of the infected file with itself, making recovery impossible. Mostly infects EXE files, although .COM files can be infected, the infection mechanism treats .COM files as .EXE files. NMAN B writes out a message, where NMAN does not. NMAN B also is nastier to the hard disk, and can erase the disk, but it is not certain if the erasure is intentional or not. It appears that this virus was written with the Borland Turbo C++ compiler, that's why this virus is sometimes called "C virus". Virus sample examined had a date of 9/24/91, so virus is at least that old.		

Name: No Bock		
Aliases: No Bock	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: No Frills		
Aliases: No Frills	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:** 835	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: No_Smoking		
Aliases: No_Smoking	**Type:** Program.	
Disk Location: COM application.	**Features:** EncryptedSends NetWare messages.Files longer than 59860 byte could not be infected.	
Damage: No intentional damageVery small files are corrupted	**Size:** 1575 byte , self-encrypting COM file.	**See Also:**

Notes: 1. The virus is not a memory resident, but leaves part of its own Int 21h in the memory as means of infecting more files.
2. On infection, it intercepts Int 21h and Int 24h to call trigger routines and to prevent DOS error messages.
3. Upon the execution of an infected file, control is passed to the virus decryption routine (the virus encrypts itself twice, thus two decryption routines are required). Using Int 21h and Int 24h, the infection routine is called which scans the directory to locate 5 uninfected COM files. It writes the body of the virus at the end of the file and modifies file entry point to JMP instruction to the starting location of the virus code.
4. The virus checks for file length and somehow it does not check the length properly. This shortcoming on the virus part causes the corruption of very small files and the very large files are exempted from infection (more than 59860 byte).
5. The trigger routine is activated on Novell NetWare stations, only. The trigger routine is called when there is an Int 24h call on infection. Upon activation, the first step is to obtain the sever name to which the infected stations connected using "GET FILE SERVER INFORMATION" function. The name of the server that was used at login will returned to virus. Second, the virus finds out the number of user connected to the server using "GET FILE SERVER INFORMATION", and obtains the hosting computer number using "GET CONNECTION NUMBER, Int 21h, AH=DCh". Third, it randomly selects two connected computers on the network, gets their names and addresses via "GET CONNECTION INFORMATION". Finally, the virus generates the phrase "NAME: Text" where NAME is the name of the network of the first selected computer. Text is a string that is send to the second selected computer. The text string is " Friday I'm in LOVE!" or "No Smoking, please! Thanks.". Receiving this type of message does not rise any suspicion, since it has the appearance of a joke making its way over the network. Eventually, the message will be received by all users and people will be alarmed to the situation.
6. The virus corrupts those EXE file with COM extension such as the compression of COM files with certain versions of DIET.
7. The recommended method for disinfection is to Re-Boot from write-protected system diskette. Identify and replace the infected file, which should be easy, knowing the type being COM and virus adds 1575 byte to any infected file.

Name: Nomenklatura			
Aliases: Nomenklatura, 1024-B,	**Type:**		
Disk Location:		**Features:**	
Damage:		**Size:**	**See Also:** Diamond
Notes: Diamond is a relative of this virus			

Name: Nostardamus		
Aliases: Nostardamus	**Type:** Program.	
Disk Location: EXE application.COM application.Program overlay files (OVL).	**Features:** Memory resident; TSR.EncryptedPolymorphic	
Damage: Displays messagesCorrupts boot sectorCorrupts a data file.Corrupts keyboard inputs.	**Size:** 2247 byte long.	**See Also:**

Notes:

The following notes are extracted from VB, March 1995:
This virus has spread in many Russian towns as was reported by Fidonet echo.
Nostardamus is a polymorphic file infector. The code has several main instruction which are selected randomly from a list. The virus has several trigging routine, each routine performs a specific task such as displaying messages, overwriting files, changing file attributes, erasing boot sectors, disabling several keys on the keyboard. Furthermore, it has instruction to elude several ' Russian' anti-virus programs.
The virus intercepts Int 21h, Int 16h, Int 1Ch, and Int 24h handler and uses their functionality rather well to perform its task smoothly and unobstructively.
Upon the execution of an infected file, control is passed to the decryption loop, and the virus body code is restored to the executable form. First, the virus uses Int 21h function to determine weather its memory resident. If its a memory resident, then CL register returns 4Bh. Otherwise, the virus acquires an area of memory for itself. It achieves that by direct manipulation of MCB chain, hooks Int 16h and Int 21h, obtains the original address of Int 21h, then returns control to the host file.
When a file is targeted for infection, the routine hooks to Int 24h to suppress any DOS error messages which occurs in write-protected disk, then it disables the Control-Break interruption and checks the extension. If the file extension is *.?YS, the virus aborts the infection routine. If the extension is ?OM or ?XE or ?VL, then infection takes place. For EXE and COM files, the virus checks the name for strings CO*, *EB, *NF, *TI,and AI*. The string CO* identifies the COMMAND.COM and the infection routine is aborted. The other strings are to identify Russian anti-virus programs WEB, ADINF, ANTI,and AIDSTEST in which case the virus turns on a special flag acknowledging that existence of these programs and how to elude them when the infected files are executed.
Files with extension EXE, COM , and OVL will be affected by virus. The virus will not infect files shorter than 1500 byte. For COM files longer than 63288, the infection routine will be aborted. When these conditions are met the virus checks the file for ' Identification Bytes' so that multiple infection is avoided. The ID for an infected EXE files is the word at offset 12h being 07B7h. And, the ID for an infected COM file is 4the byte having a value of C3h. If the file is not infected, then an encrypted virus code will be appended to the file end with jump instruction to the virus code. Then, control is returned to the host file. Also, all infected files are marked with a second ID, namely, the seconds filed of the time and date stamp to 20.
Nostardamus has several payload. When the 20 th infection occurs, the virus becomes active. First, the date is checked, If the day number equal 2* month number, the following message is display:

```
 THE NOSTARDAMUS-Erace (c) v2.1 beta
  Formatting Disk C:
   40 Mb
```

Next it simulated disk formatting (not actually erasing or formatting). Pressing any key causes a system crash. Another triggering routine is system time counter. If minute vales is less than 4, the 80 th sector of A:drive will be erased. If time is later than 18:00 , the virus hooks Int 1Ch and displays the following message:

```
    HOME RUN !!
```

Another triggering routine is placed in virus' Int 16h. The virus checks the keyboard input; It disables F8, Shit-F8, and Ctrl-F8. It Ctrl-F10 key will replace by F8 key. The last triggering routine is placed in the virus' Int 21h handler. If the file attributes is Hidden, then the virus changes its attributes to Read-only/Hidden, and overwrites the first byte with the virus name.first byte (excludes EXE, COM, SYS, and OVL files).

Name: NOTROJ		
Aliases: NOTROJ	**Type:** Trojan.	
Disk Location: NOTROJ.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.Attempts to format the disk.	**Size:**	**See Also:**
Notes: All outward appearances indicate that the program is a useful utility used to FIGHT other trojan horses. Actually, it is a time bomb that erases any hard disk FAT table that IT can find on hard drives that are more than 50% full, and at the same time, it warns: "another program is attempting a format, can't abort! After erasing the FAT(s), NOTROJ then proceeds to start a low level format. Delete the NOTROJ.COM Application.		

Name: Novell		
Aliases: Novell, Jerusalem variant	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Deletes or moves files.	**Size:** 1806-1816	**See Also:**
Notes: This virus can infect Novell lans and defeat LAN privilages. It behaves like the Jerusalem B virus in stand alone mode, loads a TSR and hooks init 21. In a networked system it hooks init 21 and 8. Once in memory, it infects files when they are run. The virus infects NetWare 2.15C servers from infected nodes, dos server writing without write privileges, server deleting without delete privileges. Server deletion can be done from nodes with just ROS privileges (i.e. neither modify flags or write). On Friday the 13th, the program deletes any executed program instead of infecting it, even from nodew with no delete privilages on the server. Files increase by a little over 1800 bytes. Date and time stamps change on files on a server, even when the node does not have the modify privilage. "sUMsDos" string in executable file. Standard detectors will probably see it, it looks like Jeruseleam-B, "sUMsDos" string in virus. Standard eradicators that can fix Jeruseleam B, though you should replace .exe and .com files.		

Name: November 17		
Aliases: November 17, 855, Nov 17, Nov. 17, Nov 17-768, Nov 17-880, Nov 17-B, Nov 17-800, (not really) Simplistic File Infector	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR above TOM.	
Damage: Erases the Hard Disk.	**Size:** 855786880928800	**See Also:**
Notes: The Nov. 17 virus is a memory resident virus that adds 855 bytes to .COM and .EXE files. It was discovered Dec, 1991 in Italy. On Nov. 17 it activates and trashes the hard disk. May target the McAfee programs SCAN and CLEAN to not infect those programs Use a scanner such as FPROT, ViruScan, IBM Scan, Novi, CPAV, NAV 2.1+, Vi-Spy, AllSafe, ViruSafe, Sweep, AVTK, VBuster, Trend, Iris, VNet, Panda, UTScan, IBMAV, NShld, Delete the file or repair with a scanner. Someone once (11/18/93) referred to this virus as "Simplistic File Infector" virus, but that is not a recognized alias for this virus. v6-140: At least 8 known variants. v6-142: correction: there are at lease 11 variants now.		

Name: November 30		
Aliases: November 30, Jerusalem variant	**Type:** same as Jerusalem	
Disk Location:	**Features:**	
Damage: same as Jerusalem	**Size:**	**See Also:**
Notes: a variant of Jerusalem with a trigger date of November 30, discovered in January 1992 Could be same virus found early last summer in Korea. (source: virus-l, v5-069)		

Name: Npox.1482		
Aliases: Npox.1482, Varicella	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-146: This virus was written to hurt users of the TBCLEAN antivirus package. If you have a file infected with the Varicella virus, and if you tried to clean this virus infected file with tbclean, what would actual happen is that tbclean will report "that this file is not infected by a virus" but what _actually_ happen was that the virus escaped the controlled environment that tbclean setup to try to disinfect the file, and the virus will go resident and hook interrupts 21h,13h,8h,1ch. and it will allocate memory under the TOM, and fool tbclean in reporting that no virus is in the file, and tbclean will exit normally! whereby, in fact the varicella virus went resident and is now infecting the system. and to advice you, the varicella virus is fairly a stealth virus that disinfects files on the file, when opened and reinfects them when closed, and it hides its virus length very well! such a virus can easily get out of control on a huge level.		

Name: NukePox		
Aliases: NukePox, NPox	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Varicella
Notes: v6-151: At least one anti-virus program can detect and remove Npox (955, 1482, 1722 and 1723)		

Name: Number of the Beast		
Aliases: Number of the Beast, Beast C, Beast D	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 512 bytes	**See Also:**
Notes: Beast: 13 variants, all of them detected (inapproiately) as 512 by SCAN 97, some of the variants are not very widely spread in Bulgaria. Variants: Beast B, C, D, E , F, and X SCAN 97 still says that "number of the beast" is the 512 virus (erroneously) v6-149: "elegant and full of tricks, but doesn't seem to spread well - not everybody seems to be running DOS 3.3"		

Name: Nygus		
Aliases: Nygus	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Nygus (163, 227, 295)		

Name: Nympho		
Aliases: Nympho	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Off-Road		
Aliases: Off-Road	**Type:** Program.	
Disk Location: COM application.	**Features:** Encrypted	
Damage: Hooks INT-08h	**Size:** 894 bytes	**See Also:**
Notes:		

Name: Ohio		
Aliases: Ohio, Den-Zuk 2, Den Zuk 2	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes:		

Name: OK		
Aliases: OK	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Omega		
Aliases: Omega	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A friday the 13th time bomb virus		

Name: One_half			
Aliases: One_half, one half, Freelove, Slovak Bomber, Explosion-II	**Type:** Multipartite.		
Disk Location: Hard disk partition table.EXE application.COM application.		**Features:** Memory resident; TSR.EncryptedStealthPolymorphic	
Damage: Encrypts the HDTrashes the hard disk.		**Size:** Polymorphic: each infection different3544 bytes long	**See Also:** Commander_Bomber

Notes: We have determined that the virus is highly infectious, and it is multiply encrypted. It infects .COM, and .EXE files, and the master boot record, and it probably infects other executable files as well. It is a stealth virus, which actively hides its infection in the boot sector. It may also hide its infections on files.
It appears to only infect .EXE and .COM files that reside on networked drives.

When activated by running an infected program, the virus modifies the master boot record on the hard disk so that it runs the virus code, which is placed in the last seven sectors of the first track on the hard disk. The eighth sector from the end of the track contains a copy of the original master boot record. The last sector of the first track contains the following clear text at the end:

Did you leave the room ?

The virus uses stealth to hide the boot infection.

According to VB of October 1994, the virus has two trigger routines. The first trigger routine is complex and attempts to executing this routine fails. Calling this complex routine leads to the encryption of DOS partitions of the hard disk. When the virus is removed the disk partitions are removed and the hard disk is trashed. The second trigger routine is called when the virus is installed in system memory. This routine test the system timer value against its own generation count routine. When these condition are to its liking then the following message is displayed:

Dis is one half.
Press any key to continue .....

and waits for response from the user. This routine is one that has the text string " Did you leave the room? ".

The virus has an error in it that causes damage to large capacity hard disks. The virus appears to make some assumptions about the file system, which causes it to write things to the wrong place if you have a larger disk with a lot of logical read/write heads. Many of the new, larger disk drives map the true number of heads and cylinders on a disk to a larger number of logical heads and fewer logical cylinders to get around some DOS limitations on the number of cylinders allowed on a disk. It appears that disks with 32 or more heads may be at risk.

The virus encrypts two cylinders of your hard drive starting with the highest numbered cylinders, every time your machine is booted, and then masks that encryption by decrypting any file accesses to that area. If the virus is not in memory, you will see encrypted data there. If you remove the virus from the disk, the encryption key is lost and the cylinders can not be disinfected. Any important files must be copied out of those cylinders before removing the virus.

The program chk_half.zip is available from DDI to find and remove this virus.
DataPhysician Plus 4.0E should detect and remove it.

DOE Virstop can decrypt the cylinders.
Norton has a special copy of NAV that can decrypt the sectors.

Note: The virus code is at a constant off-set from the file end. Therefore, the scanner can detect the virus by checking the end file not the header.

=====

Name: Ontario			
Aliases: Ontario	**Type:**		
Disk Location:		**Features:** Polymorphic	
Damage:		**Size:** Polymorphic: each infection differentIt toggles one bit only	**See Also:**
Notes:			

Name: Oropax		
Aliases: Oropax, Music, Musician	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 2756 -2806 Increase is divisible by 51	**See Also:**
Notes: Infects .COM files. After 5 minutes, the virus will start to play three melodies repeatly with a 7 minute interval in between. This can only be stopped with a reset. After 5 minutes, the virus will start to play three melodies repeatly with a 7 minute interval in between. This can only be stopped with a reset. Typical texts in Virus body (readable with HexDump facilities): "????????COM" and "COMMAND.COM" v6-151: At least one anti-virus program can detect and remove Oropax (B and C)		

Name: Osiris		
Aliases: Osiris	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Oulu		
Aliases: Oulu, 1008, Suomi	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Not very widespread in Finland		

Name: Override		
Aliases: Override	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: PACKDIR		
Aliases: PACKDIR	**Type:** Trojan.	
Disk Location: PACKDIR.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: This utility is supposed to "pack" (sort and optimize) the files on a [hard] disk, but apparently it scrambles FAT tables. (Possibly a bug rather than a deliberate trojan?? w.j.o.)		

Name: Paris		
Aliases: Paris, France	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Parity		
Aliases: Parity	**Type:** Program.	
Disk Location: COM application.COMMAND.COM	**Features:** Direct acting.	
Damage: Interferes with a running application.	**Size:** 441	**See Also:** Parity 2
Notes: Whenever an infected program is run, it infects one .COM application. The virus may emulate a parity error, display PARITY CHECK 2 and hang the machine. v6-151: At least one anti-virus program can detect and remove Parity.B.		

Name: Parity 2		
Aliases: Parity 2, Parity Boot, Parity_Boot.A and Parity_Boot.B	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.Stealth; actively hides from detection.	
Damage: Display message 'PARITY CHECK' and Halts the computerPerforms soft reboot and warm reboot.	**Size:** Overlays boot sector, no increaseReduces DOS memory by 1 kbyte	**See Also:** Parity

Notes:
A memory resident boot virus that infects floppy disk boot records and hard disk partition tables.
The Virus uses stealth techniques to hide.
Stealth techniques preclude disk scan when virus is in memory.
It may display the message PARITY CHECK and then hang the computer.
v6-149: "...Germany is full of it. Not because it is stealth or survives warm reboot (which it is and does), no - because some large warehouse has distributed it on the computers they sold...."

Updated information:
Parity_Boot.A and Parity_Boot.B are two similar Boot Sector viruses. The only difference is that 'A' version stores a copy of the original Master Boot Sector in Sector 14, Side 0, Cylinder 0 of the hard disk. While the 'B' version uses Sector 9, Side 0, Cylinder 0. This difference is important for disinfection purposes.

A hard disk is infected upon booting from an infected floppy disk. The virus examines the MBS to determine whether the disk is infected or clean. If the offset 01BCh has a value of C9h, then the hard disk is infected. If the test fails, then the virus starts the infection process. It stores parts of the 24-hour timer for later use. And it stores the address of the current Int 13h handler and reduces DOS memory by 1 kbyte, which is used for the virus code. Then, it hooks Int 13h and Int 09h. Finally, It executes a soft reboot using the Int 19h function. The reboot will use the virus' Int 13 h and Int 09h functions which loads the original boot sector into memory and gives it control.

The virus' payload is activated by Int 09h. Whenever Int 09h is called and the clock count byte stored at booting is less than the current time value, the payload will be delivered. It consists of displaying the message 'PARITY CHECK' and the processor is halted with HLT instruction, and the only way out of the situation is to turn the machine off! Also, when Ctrl_Alt_Del keys are pressed, then the virus simulates a memory parity error, executing a warm reboot.

Name: Particle Man		
Aliases: Particle Man	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: PC Flu 2		
Aliases: PC Flu 2	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove PC-Flu.		

Name: PC Weevil		
Aliases: PC Weevil	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** MTE
Notes: A mutation Engine (MTE) variant which will, like Tremor, disable Microsoft Anti-Virus (VSAFE)		

Name: PCW271		
Aliases: PCW271, PC-WRITE 2.71	**Type:** Trojan.	
Disk Location: "PCW271.???"	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 98274 Size of bogus PC-WRITE normal is 98644 bytes.	**See Also:**
Notes: A modified version of the popular PC-WRITE word processor (v. 2.71) that scrambles FAT tables. The bogus version of PC-WRITE version 2.71can be identified by its size; it uses 98,274 bytes whereas the good version uses 98,644.		

Name: Peach		
Aliases: Peach	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-122: searches for and distroys all CHKLIST.CPS files in every directory before infection takes place (thereby disabling CPAV)		

Name: Peanut		
Aliases: Peanut	**Type:** Multipartite.	
Disk Location: Hard disk boot sector.Floppy disk boot sector.COM application.	**Features:** StealthAny file start with "M" is not infected.	
Damage: No damage, only replicates.	**Size:** The virus code is 444 byte. The body is appended to end of COM file. Patches the beginning of files with "M".	**See Also:**

Notes:
The virus is transmitted to the PC by booting from an infected floppy disk and its designed to propagate. Its first action is determine whether the hard disk is infected. If the disk is clean, then the virus copies the MBS to sector 2, head 0,track 0, and installs itself in the MBS location. When this task is completed the virus loads the original MBS of the hard disk (not the boot sector of the floppy). This action gives the illusion that the user has booted from the hard disk and a person may not realize that a floppy disk was used in the booting the system just because it was left in A drive. By now the virus has installed its own Int 13h handler and its ready to propagate.

The infection process starts when the user executes a file. When the file is loaded by reading sectors, Peanut starts its second task which is to identify file marker and type. If a file starts with an "M ", the virus identifies the file as an EXE file and installs its own Int 21h handler and remaps the original Int 21h into Int B9h. The file will not be infected and normal processing will resume. If the file does not start with an "M", then Peanut assume its a COM file. In this instant, the virus will paths its beginning with an "M" followed by jump to the end of file. It appends the rest of the code to the file end. The virus stores the first four byte of the original COM file for patching back later, also it preserves the time and date of the file and intercepts Int 24h from now on.

On an infected PC, all floppy reads are intercepted. The boot sector are overwritten by Peanut and the disk will infected (for infected floppy disks, it will be re-infected).For write-protected disk, the user is lead to believe that every thing is OK, since, the user will not receive any critical error message.

This virus has stealth characteristic; all reads to MBS are intercepted and the original MBS is returned . Any write to MBS are ignored without notifying the user.

So far, this virus seams to have no payload other than replication.

For disinfection, the VB recommended the following procedure:
Under clean system conditions, use the FDISK/MBR command to install the original MBS.
Infected files should be identified and removed.

Name: Pentagon		
Aliases: Pentagon	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**

Notes: It infects floppy disk boot sectors, and removes the Brain virus from any disk it finds. The virus can survive a warmboot.

It appears that no anti-viral researchers can get this virus to replicate.

Name: Perfume		
Aliases: Perfume, 765, 4711	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 765	**See Also:**
Notes: It infects .COM files, and after 80 executions, it demands a password to run the application. The password is 4711 (the name of a perfume). A password request for a program that does not need one, or the printing of code on the screen when a program is run, much like using the DOS TYPE command with an excutable file. One version contains the following strings: "G-VIRUS V2.0",0Ah,0Dh, "Bitte gebe den G-Virus Code ein : $" <CRLF> 0Ah,0Dh,"Tut mir Leid !",0Ah,0Dh,"$"; (translated 2nd and 3rd strings: "please input G-virus code"; "sorry") Another version has a block of 88(dec) bytes containing 00h.		

Name: Perry		
Aliases: Perry	**Type:** Vaporware Virus; not real.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: There is a false positive report of the Perry virus as reported by CPAV 2.0 on VALIDATE.COM, dist. by Patricia Hoffman as part of VSUM package. Perry is NOT A VIRUS. Perry is a program which was used to ask for a password when run, or self-destruct on a specific date, it is not and never was a virus.		

Name: Phoenix		
Aliases: Phoenix, P1	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR above TOM.EncryptedPolymorphic	
Damage:	**Size:** 1704 All .COM files but COMMAND.COMIt overlays part of COMMAND.COMMulti ple infections are possible.Polymorphic: each infection different	**See Also:**
Notes: The Phoenix virus is of Bulgarian origin. This virus is one of a family of three (3) viruses which may be referred to as the P1 or Phoenix Family. The Phoenix virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. Phoenix infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. Phoenix is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,704 bytes of viral code being appended to the file. Systems infected with the Phoenix virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with Phoenix memory resident will result in a warm reboot of the system occurring, however the memory resident version of Phoenix will not survive the reboot. The Phoenix Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples. Also see: PhoenixD, V1701New A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files v6-123: Phoenix.800 Disables Ctrl-Break checking		

Name: Phoenix D		
Aliases: Phoenix D, P1	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.COMMAND.COM.	**Features:** Memory resident; TSR above TOM.EncryptedPolymorphic	
Damage:	**Size:** 1704 All .COM files but COMMAND.COMIt overlays part of COMMAND.COMMulti ple infections are possible.Polymorphic: each infection different	**See Also:**

Notes: The Phoenix-D virus is of Bulgarian origin, and is a bug fixed version of Phoenix. This virus is one of a family of three (3) viruses which may be referred to as the P1 or Phoenix Family. The Phoenix virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. Phoenix infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. Phoenix is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,704 bytes of viral code being appended to the file. Systems infected with the Phoenix virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with Phoenix memory resident will result in a warm reboot of the system occurring, however the memory resident version of Phoenix will not survive the reboot. The Phoenix Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples.
Also see: Phoenix, V1701New
A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files

Name: Phx		
Aliases: Phx	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: v6-151: At least one anti-virus program can detect and remove this virus.

Name: Ping Pong		
Aliases: Ping Pong, Bouncing Ball, Italian, Bouncing Dot, Vera Cruz, Turin Virus	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**

Notes: Bouncing dot appears on screen. No other intentional damage. Spreads between disks by infecting the boot sectors.
The bootsector contains at the offset 01FCh the word 1357h.
Enter TIME 0, then immediately press any key and Enter; if the virus is present, the bouncing dot will be triggered
v6-137: well written virus, it jumps to top of memory, doesn't work with 80286 and higher

Name: Ping Pong B		
Aliases: Ping Pong B, Boot, Falling Letters	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Bouncing dot appears on screen. No other intentional damage. Spreads between disks by infecting the boot sectors.		

Name: Pit		
Aliases: Pit	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Pixel		
Aliases: Pixel, V-847, 847, V-847B, V-852, Amstrad, Advert, Near_End, Pojer	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 847	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file. v6-151: At least one anti-virus program can detect and remove Pixel (277.B, 300, 343, 846, 847.Advert.B, 847.Advert.C and 847.Near_End.B) Pojer.1935 (only COM files - EXE files are not infected properly, the virus code is only appended)		

Name: PKFIX361		
Aliases: PKFIX361	**Type:** Trojan.	
Disk Location: PKFIX361.EXE	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: PKFIX361.EXE *TROJAN* Supposed patch to v3.61 - what it really does is when extracted from the .EXE does a DIRECT access to the DRIVE CONTROLLER and does Low-Level format. Thereby bypassing checking programs. (This would be only XT type disk drive cards. w.j.o.)		

Name: PKPAK/PKUNPAK 3.61		
Aliases: PKPAK/PKUNPAK 3.61, PK362, PK363	**Type:** Trojan.	
Disk Location: PK362.EXEPK363.EXEPKPAK/PKUNPAK v. 3.61	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: PKPAK/PKUNPAK *TROJAN* There is a TAMPERED version of 3.61 that when used interfers with PC's interupts. PK362.EXE This is a NON-RELEASED version and is suspected as being a *TROJAN* - not verified. PK363.EXE This is a NON-RELEASED version and is suspected as being a *TROJAN* - not verified.		

Name: PKX35B35		
Aliases: PKX35B35, PKB35B35	**Type:** Trojan.	
Disk Location: PKX35B35.ARCPKB35B35.ARC	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: PKX35B35.ARC, PKB35B35.ARC This was supposed to be an update to PKARC file compress utility - which when used *EATS your FATS* and is or at least RUMORED to infect other files so it can spread - possible VIRUS?		

Name: PKZIP Trojan 1		
Aliases: PKZIP Trojan 1, ZIP Trojan, PKZ201.ZIP, PKZ201.EXE	**Type:** Program; activates when run.	
Disk Location: PKZ201.ZIP, PKZ201.EXE	**Features:** Direct acting.	
Damage: Alpha level software, anything is possible.	**Size:**	**See Also:** PKZIP Trojan 2
Notes: The PKZIP trojan 1 is PKZIP version 1.93 Alpha renamed as PKZIP version 2.01. The only danger, is that this is alpha level software, and may have bugs in it. There will never be a version of PKZIP numbered 2.01 though there may be a version 2.0 in the near future (6/92). The program has been found in the files PKZ201.ZIP, PKZ201.EXE and has been uploaded to several BBSs. Contact PKWARE if you see it. Voice at 414-354-8699, BBS at 414-354-8670, FAX at 414-354-8559 PKWARE Inc., 9025 N. Deerwood Drive, Brown Deer, WI 53223 USA See also PKZIP Trojan 2 Check the version number using PKUNZIP with the -l option to list the contents of the archive. If it is version 2.01 then delete it. Delete the file.		

Name: PKZIP Trojan 2		
Aliases: PKZIP Trojan 2, PKZIPV2.ZIP, PKZIPV2.EXE, ZIP Trojan	**Type:** Trojan.	
Disk Location: PKZIPV2.ZIPPKZIPV2.EXE	**Features:**	
Damage: Erases the Hard Disk.	**Size:** The files are short, only a few lines of text.	**See Also:** PKZIP Trojan 1
Notes: The PKZIP trojan is a program masquareding as PKZIP version 2.2. It is actually just a short command file containing DEL C:\DOS*.*, and DEL C:*.* . When run, it attempts to erase the contents of the C:\DOS directory and the c:\ directory. There will never be a version of PKZIP numbered 2.2 though there may be a version 2.0 in the near future (6/92). The Trojan has been found in the files PKZIPV2.ZIP, PKZIPV2.EXE and has been uploaded to several BBSs. If you have had files deleted by this Trojan, you may be able to recover them with an unerase utility such as those supplied with Norton Utilities or PCTools. Contact PKWARE if you see it. Voice at 414-354-8699, BBS at 414-354-8670, FAX at 414-354-8559 PKWARE Inc., 9025 N. Deerwood Drive, Brown Deer, WI 53223 USA See also PKZIP Trojan 1 Your hard disk is erased. Type the file to see if it is a command file instead of an executable. The command file will contain instructions to delete files on the hard disk. Delete the file.		

Name: Plague		
Aliases: Plague	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: claim that it was created by either someone in Brisbane Austrailia, or USA. (virus-l, v5-189)		

Name: Plastique		
Aliases: Plastique, 3012, HM2, Plastique 1, Plastique 4.51	**Type:** Boot sector.	
Disk Location: COM application.EXE application.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:** Jerusalem, Anticad
Notes: Most variants play a melody, if you press Ctrl-Alt-del while melody is being played, it overwrites the beginning of the hard disk.		

Name: Plovdiv		
Aliases: Plovdiv, Plovdiv 1.1, Plovdiv 1.3, Damage 1.1, Damage 1.3, Bulgarian Damage 1.3	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR above TOM.	
Damage: Corrupts a program or overlay files.Attempts to format the disk.	**Size:** Overlays application, no increase1000 bytes in files, 1328 bytes in memory	**See Also:**
Notes: The virus identifies infection by the seconds field in file time. It allocates a memory block at high end of memory, 1344 bytes long Programs are infected at load time (using the functionload/execute of MS-DOS) and whenever a file is opened with the extension of .COM or .EXE The virus carries an evolution counter that is decreased every time the virus is executed. At 0, virus reads system timer, if the value of hundreds > 50 virus will format all available tracks on current drive (effectively 50% chance of destruction) The virus knocks out the transient part of COMMAND.COM forcing it to be reloaded and thereby infected, therefore it is a "fast infector" contains string "(c)Damage inc. Ver 1.3 1991 Plovdiv S.A."		

Name: Pogue		
Aliases: Pogue	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Unknown, not analyzed yet.	**Size:** Polymorphic: each infection different	**See Also:**
Notes: A variant of Gotcha that uses the MtE mutation engine.		

Name: Possessed		
Aliases: Possessed, Possessed A, Possessed B, Demon	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Deletes or moves files.	**Size:**	**See Also:**
Notes: Displays a low resolution picture of a demon on the screen with the words "Your computer is now Possessed" under it. Can delete files This virus has been falsely identified within one of the files on the DayStar Digital LT200 PC LocalTalk software disk (file DNET2.COM) by an older version of McAfee's SCAN82. If a "positive" reading is done on this file, please confirm by using a newer version of the software, or another scanning package.(virus-l, V4-214) standard detection/eradication packages		

Name: Print Screen		
Aliases: Print Screen, 8920, EB-21, Print Screen 2, PrtSc	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: VirHunt calls it PrtSc		

Name: Prot-T.Lockjaw.2		
Aliases: Prot-T.Lockjaw.2, LOKJAW-ZWEI, Lockjaw-zwei, Black Knight	**Type:** Companion program.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: v6-124: Author calls it Lockjaw-zwei, (zwei is two in German), CARO name is Prot-T.LockJaw.2. The author calls it Lockjaw-zwei (not zwie; "zwei" means "two" in German); standard CARO name is Prot-T.LockJaw.2. It's a companion resident virus. It targets several anti-virus products, meaning that it deletes files with particular names if they are executed with the virus active in memory. After deleting the file(s), the virus displays a visual effect. In particular, those names are: *IM.* (Integrity Master) *RX.* (VirX PC) *STOP.* (VirStop) *AV.* (CPAV, MSAV) *PROT.* (F-Prot) *SCAN.* (SCAN) *LEAN.* (CLEAN)		

Name: Proto-T.Flagyll.371		
Aliases: Proto-T.Flagyll.371	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 371	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: proton		
Aliases: proton	**Type:** Program.	
Disk Location: EXE application.COM application.COMMAND.COM	**Features:** Memory resident; TSR.	
Damage:	**Size:** 4000 bytes	**See Also:**
Notes:		

Name: Proud		
Aliases: Proud, V1302, Phoenix related	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: PS-MPC		
Aliases: PS-MPC, Alien, Arcv-9, Deranged, Dos3, Ecu, Flex, Geschenk, Grease, Iron Hoof, Napolean, Nirvana, Nuke5, Page, Shiny, Skeleton, Soolution, Sorlec4, Sorlec5, Soup, T-rex, Toast, Toys, McWhale, Jo, Scroll, Slime	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove PS-MPC (331, 349, 420, 438, 478, 481, 513, 547, 564, 574, 578, 597, 615, 616, 1341, 2010, Alien.571, Alien.625, Arcv-9.745, Arcv-10, Deranged, Dos3, Ecu, Flex, Geschenk, Grease, Iron Hoof.459, Iron Hoof.462, Napolean, Nirvana, Nuke5, Page, Shiny, Skeleton, Soolution, Sorlec4, Sorlec5, Soup, T-rex, Toast, Toys and McWhale.1022)		

Name: PSQR		
Aliases: PSQR, 1720	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Jerusalem
Notes: v6-151: At least one anti-virus program can detect and remove this Jerusalem variant		

Name: QRry		
Aliases: QRry, Essex	**Type:** Boot sector.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-139: the boot sector has the word "QRry" in it. V6-142: FPROT calls it QRry, it's an MBR infector, so FDISK /MBR will remove it.		

Name: Quadratic		
Aliases: Quadratic	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Quadratic.1283.		

Name: Quicky		
Aliases: Quicky, Quicksilver.1376, V.1376	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.Encrypted	
Damage: Deletes checksum data files.	**Size:** 1376 bytes long	**See Also:**

Notes:
The following notes are extracted from VB, June 1995:
Quicky appeared in UK and Europe. The virus is 1376 bytes long and it infects EXE files. Quicky uses no stealth techniques to hide its present, the increase in file length can be detected immediately.
The virus code is poorly written and have many flaws. The writer had attempted to include a destructive routine that could corrupt writes to the hard disk, however, the writer was not successful in his programming so he/she had bypassed that section with a jump.

The first action of the code is to decrypt its code.It is decrypted to two halves using a simple byte-swapping XOR routine. It re-modifies its decryption routine and patches its addressing to identify its location in memory. Now, the first error/bug in the code shows up. The virus checks to see if its already a memory resident by calling Int 21h with AX=C000h (a memory resident copy returns AX=76F3h). This call conflicts with some interrupt calls of ' NetWare' so it may lead to aborting the host program). Next, it checks the continent of register BX for a certain vale. This check is to activate the destructive routine which is currently is bypassed. If the virus is memory resident, then control is returned to the host program. Otherwise it move down to memory, hooks Int 13h and Int 21h, returns control to the host program.

The file infection method is somewhat unusual. It looks out for program execution on the system, then it remove read-only attribute, open the file, closes the file immediately, reset the attributes, and lets the program to run. The virus infects the program during the closing process The net effect of this method is that even write-protected files become infected upon their execution (due to programing error, DOS error messages are displayed when the infection process fails).

Quicky has a section that deletes various checksum data files used by anti-virus programs to prevent detection. Again, due programming error, data files are deleted from the current directly only which may not be the same directory that contains the infected program. This error allows the detection of the virus by checksummer after all.

The recommended method for disinfection is to use clean system conditions, then identify and replace the infected files.
The memory resident copy can be deactivated by calling Int 21h with AX=C001h.

Name: QUIKRBBS		
Aliases: QUIKRBBS	**Type:** Trojan.	
Disk Location: QUIKRBBS.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**

Notes: This Trojan horse advertises that it will install program to protect your RBBS but it does not. It goes and eats away at the FAT.

Name: QUIKREF		
Aliases: QUIKREF	**Type:** Trojan.	
Disk Location: ARC513.COM	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**
Notes: This ARChive contains ARC513.COM. Loads RBBS-PC's message file into memory two times faster than normal. What it really does is copy RBBS-PC.DEF into an ASCII file named HISCORES.DAT.		

Name: Quox		
Aliases: Quox, Stealth 2 Boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** Stealth	
Damage: Corrupts floppy disk boot sectorOverwrites sectors on the Hard Disk.No damage, only replicates.	**Size:** Overlays boot sector, no increase Installs itself in the top 1K of the base memory	**See Also:**
Notes: 1. When a system is booted from an infected disk the virus installs itself on the Master Boot Sector. Also, when a clean floppy disk is inserted into an infected machine, any attempt to access the boot sector results in infecting the disk. 2. Its known function is only replication (No deliberate damage or side effect). 3. The occupies a single disk sector of 512 bytes which replaces the Master Boot Sector of the hard disk or the DOS Boot Sector on a floppy disk. 4. The virus take advantage of the DOS FDISK program that partitions the disk. It locates the Boot Sector and installs itself. Any version of DOS that does not comply with the conventions are safe from infection, because the infection routine fails to locate the Boot Sector and its aborted. 5. When an infected 1.4 MByte 3.5-inch disks is accessed by an clean system. The disk becomes unreadable under DOS and the message " General failure error ' is given. This failure is caused by MS-DOS operating system, not the virus. 6. Disinfecting a fixed disk must be done by booting from write-protected system diskette. Using the DOS command FDISK/MBR or disk editor to restore the Boot Sector saved by the virus. Floppy disks are sanitized by reformatting the disk or by copying the boot sector from a clean disk of the exact same type. For unreadable disk, data are recovered by copying the boot sector of a clean to the infected disk.		

Name: Radyum		
Aliases: Radyum	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Radyum (698 and 707)		

Name: RAM		
Aliases: RAM	**Type:** Program; activates when run.	
Disk Location:	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: v6-081: There is no such thing as the RAM virus. Somebody gave Patty [Hoffman] a sample which was infected with two viruses - Cascade and Jerusalem, I think. This combination works perfectly together, but she did not realize the nature of the sample, and seemed to think this was one new virus. There are some other non-existing viruses in VSUM as well, but they are mostly for "copy protection" purposes.... - -frisk		

Name: Rape		
Aliases: Rape	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Rape (2777.A and 2877.B)		

Name: Rasek		
Aliases: Rasek	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Rasek (1489, 1490, and 1492).		

Name: RCKVIDEO		
Aliases: RCKVIDEO	**Type:** Trojan.	
Disk Location: RCKVIDEO.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: After showing some simple animation of a rock star, the program erases every file it can find. After about a minute of this, it creates three ascii files that say "You are stupid to download a video about rock stars".		

Name: Red Diavolyata		
Aliases: Red Diavolyata	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Red Diavolyata (830.B and 830.C).		

Name: Relzfu		
Aliases: Relzfu	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: A friday the 13th time bomb virus		

Name: Retribution		
Aliases: Retribution	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Ripper		
Aliases: Ripper	**Type:** Multipartite.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.FORMAT.COM, SYS.COM, MORE.COMUNFORMAT.COM	**Features:** Stealth	
Damage: Attempts to format the disk.	**Size:**	**See Also:** Jack-the-Ripper

Notes: This appears to be different from Jack-the-Ripper.

It lives in the boot sector of floppies and hard disk partition tables and infects four DOS files :- FORMAT.COM, SYS.COM, MORE.COM, UNFORMAT.COM .
On the sixteenth reboot, it will reformat your hard drive.

Dr Solomons Tookit also detects Ripper
CPAV v 2 (due early '94) will detect it
F-PROT

Name: RMNS		
Aliases: RMNS, RMNS MW	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** Two parts; Male (297 bytes) and Female (353 bytes)	**See Also:**

Notes:
The following notes are extracted from VB, May 1995:

The virus get its name from an internal text string at the end of the code. The virus has two parts, the male code is 297 bytes long, and the female code is 353 bytes long. The following text strings are found at end:

Male: R.M.N.S Test Virus R.M.N.S MW Man
Female: R.M.N.S Test Virus R.M.N.S MW Woman

Each section is installed separately in memory, and file infection occurs only when both section are memory resident on the same PC. The code is appended to the end of COM file with JMP VIRUS instruction at the beginning of the host file. The two codes are similar and different from each other at the same time. They both intercept Int 21h, and take control upon the execution of an infected file. The difference comes it their functionality. The male intercepts file execution. The female infects file only when asked by the male virus.

The virus places its ID in register AX. When an inquiry is make about the value of register AX, a file infected with the male part returns a value of 4BBCh, and the female part returns 4BBDh. However, both parts returns 4BBBh when they are memory resident. Also, the time date stamp of all infected files are set to 31.07.80; 12:07am.

The virus intercepts Int 21h function Load and Execute only. Both parts use the subfunctions of Load and Execute call for their communication and infection.

On a Load and Execute call, the male section checks the file and if it is a clean COM file, then it calls the female section with an ' infect it ' call (Int 21h, AX=4BB4h). The female part checks the length of the file. If its longer than 65024 bytes, infection is aborted, otherwise, the infection process takes place. The system timer is used in deciding which part to be used in the infection by this method both parts have a 50% chance of infecting files.

The virus makes no attempt to hide its present, suppress DOS error message, etc. So far its only goal is to propagate.

The recommended method for disinfection is to use clean system conditions, then identify and replace the infected files.

Name: RPVS		
Aliases: RPVS, 453, RPVS-B, TUQ	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 453	**See Also:**
Notes: Whenever an infected application is run, at least one other .COM file in the default directory is infected.		

Name: Russian_Mirror		
Aliases: Russian_Mirror	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Russian_Mirror.B.		

Name: Russian Mutant		
Aliases: Russian Mutant, 914	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Saddam		
Aliases: Saddam, stupid	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 917-924	**See Also:**
Notes: This appears to be a variant of the Stupid virus. On every eigth infection, the string: "HEY SADAM"{LF}{CR} "LEAVE QUEIT BEFORE I COME" is displayed. The virus copies itself to [0:413]*40h-867h, which means that only computers with 640KB can be infected. Many large programs also load themselves to this area and erase the virus from the memory, or hang the system.		

Name: Sampo		
Aliases: Sampo, Wllop, Turbo	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR above TOM.Display message.Over rides several MBS virus and takes controlStealthSimulates warm reboot.	
Damage: On Nov. 30, displays message.Installs 'Telefonica.A' virus under specific conditions.Sends misleading messages and plays trick on users	**Size:** Overlays boot sector, no increase	**See Also:** Stones and its variants

Notes: From VB March & April 1995 issues:

Sampo is in the wild in England and Singapore. Its is a MBS infector or Partition Table sector infector (PT) on hard disk. It acquires 6 kbyte of memory for its code, just below the 640 kbyte of the base memory. The method of installing itself is similar to any MBS virus. It stores the original MBS in sector 14 track 0.

The virus has few interesting feature; It knows several MBS viruses (Stoned is one of them) and it carries an encrypted copy of the virus 'Telefonica.A' with itself. Before installing itself, Sampo searches for there viruses and extracts any valuable information they have obtained from the system. When it install itself on the top of the memory it overwrites all the altered make by those virus, thus, it controls the system, overriding the others.

The virus is capable of surviving a warm reboot (i.e using Ctrl_Alt_Del keys). It simulates the complete process involved in the warm reboot, deceiving the user and remaining in memory.

Sampo delivers its payload on ' 30 November ' about 2 hours after booting. It displays the following message:

```
          S A  M P O
       "Project X"
  Copyright (c) 1991 by the
  Sampo X-Team. All rights
   reserved.
    University Of The East
          Manila
```

Sampo is partial to floppy disk, and it attacks them with vengeance. The memory-resident Sampo attempts to infect the boot sector of a floppy disk during any read function, such as after DIR command. First, it checks for write-protection attribute. The floppy disk will be infected readily when its not write-protected. If its write-protected, then Sampo plays trick and causes trouble. It copies an image of Telefonica.A virus to the buffer and informs the user that the boot sector is infected with Telefonica.A virus, when in reality the floppy is quit clean. This message is rather misleading for the user will try to remove a virus that does not exist on the boot sector. When the boot sector of write-protected floppy disk is copied to an infected system, the boot sector of the copy will be actually infected with Telefonica.A virus.

The recommended method for disinfection is to use FDISK/MBR command under clean system conditions.

Name: Saratoga		
Aliases: Saratoga, 632, Disk Eating Virus, One In Two	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.Corrupts the file linkages or the FAT.	**Size:** 642 to 657 Length MOD 16 will always be 0.	**See Also:**
Notes: Infects every 10th .EXE file run, and if the current drive is a hard disk larger than10M bytes, the virus will select one cluster and mark it as bad in the first copy of the FAT. Diskettes and 10M byte disks are not affected. Disk space on hard drives shrinking. .EXE files increasing in length. EXE Files: Infected files end in "PooT". System: Byte at 0:37F contains FF (hex)		

Name: Sata		
Aliases: Sata	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Sata.612.		

Name: Satan Bug		
Aliases: Satan Bug, SatanBug, Sat_Bug, Satan, S-Bug, Fruit-Fly	**Type:** Program.	
Disk Location: EXE application.COM application.COMMAND.COMProgram overlay files.?SYS System files.?	**Features:** Memory resident; TSR.Encrypted	
Damage: Corrupts a program or overlay files.	**Size:** Polymorphic: each infection differentFiles increase 2.9K to 5K	**See Also:** Natas

Notes: The virus is a memory resident, non-stealth, encrypted, mutating, polymorphic virus that infects .COM, .EXE, .SYS, and .OVL files.
It hooks the file open and file execute commands and infects programs when they are opened or executed.

If Satan Bug is not already in memory, and if COMSPEC is not the first item in the environment (SET) the virus will not load into memory. If the virus is already in memory, this has no effect. If command.com is infected there is no way to make comspec last without having the virus load first. This appears to be how the virus writer protected his own system. To move comspec from the first position, use something like the following at the beginning of your autoexec.bat file:
SET TEMP=C:\DOS
SET COMSPEC=C:\COMMAND.COM
This puts comspec into the second position. Note that if you redefine TEMP, comspec will move back into the first position.
The virus addes 100 years to the file's creation date. It probably uses this to check for an infection. You can't see this change with the DIR command, but must use a special utility. NAVCERT created the program CHKDATE to look for this change in the date.
Since the program infects .SYS files, network drivers tend to break after infection, making networks inaccessible. Note that I have not been able to get it to infect a .sys file, but it does infect emm386.exe which is usually installed high and could force the other drivers out.
Do not run an infected virus scanner on a disk, as it will then infect the whole disk.
Encrypted in the file is the text:

SATAN BUG virus - Little Loc

Locate with: DataPhysician Plus 4.0B, Scan V106, Norton AntiVirus 2.1 with August 1993 virus definitions.
Scan v106-109 do not see all infected files.

Name: Satyricon		
Aliases: Satyricon	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: SBC		
Aliases: SBC, SBC-1024	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Corrupts a program or overlay files.	**Size:** 1024min length of infectable files is 1536 bytesPolymorphic: each infection different	**See Also:**
Notes: Fairly new as of Jan 1992, an encrypted, but not polymorphic virus, memory resident, uses INT 21h/AX=4BFFh to detect its presence in memory, fast infector (infects both when copy and execute files) .EXE files are padded up to the next multiple of 16 before they are infected. Nothing obviously intentionally destructive in the virus code		

Name: Scrambler		
Aliases: Scrambler, KEYBGR Trojan	**Type:** Trojan.	
Disk Location: KEYBGR.COM	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.	**Size:**	**See Also:**
Notes: About 60 minutes after the trojan KEYBGR.COM is started a smiley face moves in a random fashion about the screen displacing characters as it moves. The Trojan contains many copies of the string "nothing".		

Name: Screaming Fist		
Aliases: Screaming Fist	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: Rumor: Written by the group PHALCON/SKISM (like Bob Ross, aka Beta virus) Some debate whether it is polymorphic or not v6-151: At least one anti-virus program can detect and remove Screaming Fist.I.683.		

Name: SECRET		
Aliases: SECRET	**Type:** Trojan.	
Disk Location: SECRET.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: BEWARE!! This may be posted with a note saying it doesn't seem to work, and would someone please try it; when you do, it formats your disks.		

Name: SECURE.COM		
Aliases: SECURE.COM	**Type:** Rumored virus, just password guesser	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: virus rumor in comp.sys.novell in July 1991. Inquiry in virus-l v4-128. From virus-l: There has been some discussion in comp.sys.novell about a new "virus" called SECURE.COM which opens up and damages netware binderies. No-one has seen it themselves yet, everyone has heard about it, so it may be another "urban legend". It is likely that if it does exist someone in this group will have heard of it, or be CERTAIN that it does not exist. It is a password guessing program		

Name: Sentinel		
Aliases: Sentinel	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: written in Pascal, created in Bulgaria		

Name: Shake		
Aliases: Shake	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Shake.B.		

Name: Shanghai		
Aliases: Shanghai	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Shifter		
Aliases: Shifter	**Type:** Boot sector.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Possibly from Russia		

Name: SI-492		
Aliases: SI-492	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove SI-492.C.		

Name: SIDEWAYS		
Aliases: SIDEWAYS, SIDEWAYS.COM	**Type:** Trojan.	
Disk Location: "SIDEWAYS.COM"	**Features:**	
Damage: Corrupts boot sector	**Size:** 3 KB SIDEWAYS.COM30 KB The legitimate SIDEWAYS.EXE application.	**See Also:**
Notes: Both the trojan and the good version of SIDEWAYS advertise that they can print sideways, but SIDEWAYS.COM trashes a [hard] disk's boot sector instead.		

Name: SillyC		
Aliases: SillyC	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove SillyC (208 and 215).		

Name: SillyOR		
Aliases: SillyOR	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Variants include versions: 60, 66, 68, 69, 74, 76, 77, 88, 94, 97, 98, 99, 101, 102, 107, 109 and 112 v6-151: Overwrites/destroys infected files.		

Name: Simulation		
Aliases: Simulation	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Sistor		
Aliases: Sistor	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Sistor (1149 and 3009).		

Name: Skew		
Aliases: Skew	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Skew.445		

Name: Slovakia		
Aliases: Slovakia	**Type:** Program.	
Disk Location: EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Only activity is infecting files, sometimes displaying a message. Infects in current directory or path. Non-resident. Infected files get increased by 2000-2200 bytes. Last four bit of length are set to 1101binary. Virus remains inactive in infected program 10 days or til the end of the month. It's an encrypted virus. Decryption code has 8 mutations. On Monday, Wed, or Friday after March 1992, message displayed: "SLOVAKIA virus version 3.00 (c) 1991-1992 by??. All Rights Reserved. Greeting from Bratislava, SLOVAKIA.Type the word SLOVAKIA: ....."		

Name: Slub		
Aliases: Slub	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Smeg		
Aliases: Smeg, Pathogen, Queeg	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Memory resident; TSR.Polymorphic	
Damage: Overwrites sectors on the Hard Disk.	**Size:**	**See Also:** Junkie
Notes: Smeg and its variants are memory resident, polymorphic COM and EXE infectors. The Pathogen variant overwrites part of your disk drive between the hours of 17:00 and 18:00 on Monday evenings. It then prints the follwoing message: Your hard-disk is being corrupted, courtesy of PATHOGEN! Programmed in the U.K. (Yes, NOT Bulgaria!) [C] The Black Baron 1993-4. Featuring SMEG v0.1: Simulated Metamorphic Encryption Generator! 'Smoke me a kipper, I`ll be back for breakfast.....' Unfortunately some of your data won`t!!!!! The author of SMEG is spending 15 months in jail for computer misuse. McAfee SCAN incorrectly detects SMEG in the Windows NT system file NTIO.SYS.		

Name: Smoka		
Aliases: Smoka	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Sofia-Term		
Aliases: Sofia-Term	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Sofia-Term (837 and 887).		

Name: Solano 2000		
Aliases: Solano 2000, Dyslexia, Dyslexia 2.00, Dyslexia 2.01, Syslexia, Subliminal	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Jerusalem
Notes: v6-151: At least one anti-virus program can detect and remove this Jerusalem variant.		

Name: Spectre		
Aliases: Spectre	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: destroys data April 1 We don't know if this is real or not. We have only a Chinese news report about it.		

Name: Split		
Aliases: Split	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:** 250 bytes	**See Also:**
Notes: infects every comfile in the currect directory. Has been found in the wild in germany.		

Name: Spring		
Aliases: Spring	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Stamford		
Aliases: Stamford	**Type:**	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes:		

Name: STAR		
Aliases: STAR, STRIPES	**Type:** Trojan.	
Disk Location: STAR.EXESTRIPES.EXE	**Features:**	
Damage: Cracks/opens a BBS to nonprivileged users.	**Size:**	**See Also:**
Notes: STAR.EXE Beware RBBS-PC SysOps! This file puts some stars on the screen while copying RBBS-PC.DEF to another name that can be downloaded later! STRIPES.EXE Similar to STAR.EXE, this one draws an American flag (nice touch), while it's busy copying your RBBS-PC.DEF to another file (STRIPES.BQS).		

Name: Stardot		
Aliases: Stardot, 805, V-801	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Stardot.789.C.		

Name: Starship		
Aliases: Starship	**Type:** Stealth virus	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Russian origin virus, infects device drivers (see also SVC 6.0 virus) Hard to get to replicate, but it will if you try hard enough can infect when copying files on diskettes, but is quite buggy		

Name: Stealth B		
Aliases: Stealth B, STB, AMSES, Stealth.B, Stelboo	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.	**Features:** StealthMemory resident; TSR.	
Damage: Corrupts floppy disk boot sectorCorrupts boot sector	**Size:** 512 bytessix sectors	**See Also:**

Notes:
The virus code is six sectors in length. It infect 360k and 1.2m floppies by formatting an extra track and placing 5 sectors of virus code followed by the original boot sector. On 720k and 1.44m floppies, however, it uses the last cluster, head 1, to store the code and boot sector, and mark these sectors as bad to protect them. On the hard drive it uses track 0, head 0, sectors 2-7 to store the additional sectors.

The virus "stealths" the infected boot sector on floppies and the infected MBR by returning an image of the stored original on disk reads. The other six sectors are stealthed on the hard drive by returning a buffer full of nulls. On floppies, however, these six sectors are not stealthed.

The virus reserves 4k of memory. Thus, on a 640k machine, running chkdsk will report 651,264 bytes rather than the normal 655,360 bytes and using debug to dump the word at 0000:0413h one will find the value 27Ch (as bytes this will appear as 7C 02). Running chkdsk on an infected 3.5 inch floppy (720k or 1.44m) will also report 3072 bytes in bad clusters.

Stealth.B does not contain any intentionally damaging code, but has been reported as wreaking havoc with some memory managers. interferes with the operation of Microsoft Windows. Starting Windows with the virus resident will simply return you to the DOS prompt and leave the system unstable. If Windows is set to 32 bit access the following message from Windows will appear:

"The Microsoft Windows 32-bit disk driver (WDCTRL) cannot be loaded. There is unrecognizable disk software installed on this computer.

"The address that MS-DOS uses to communicate with the hard disk has been changed. Some software, such as disk-caching software, changes this address.

"If you aren't running such software, you should run a virus-detection program to make sure there is no virus on your computer.

"To continue starting Windows without using the 32-bit disk driver, press any key."

Pressing a key leaves you back at the DOS prompt. This will have an obvious impact on today's Windows-dependant environments.

The virus evidently originated in the United States, in southern Florida.Alternately, Stealth.B could be a forerunner of Stealth, or they may have a common ancestor.

The virus is also called STB, AMSES, and Stelboo.

Name: Sterculius		
Aliases: Sterculius	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Sticky		
Aliases: Sticky, Nu_Way ,Multi2, Fist.927	**Type:** Multipartite.	
Disk Location: EXE application.COM application.Hard disk boot sector.	**Features:** Memory resident; TSR.EncryptedInfects COM files of 300 - 62000 bytes.All files with SCAN name are exempt from infection.	
Damage: No damage, only replicates.	**Size:** 927 bytes long	**See Also:** Tequila

Notes: The following notes are extracted from VB, July 1995:

Sticky was found in the Midwest USA. The virus was referred to by virus names, many of the names having the string 'Fist' or 'Scream'. Sticky should not be confused with 'Screaming_Fist' Family, because they differ in functionality and the code does not contain the text 'Screaming_Fist'.

Hard disk infection occurs upon the execution of infected file on the system. The virus drops into MBS using Int 13h. Later, when the system is rebooted, the virus become memory resident. It acquires 3k just under the 640k limit (CHKDSK shows the lower amount of memory available). Now, the memory resident copy is ready to perform its task.

The memory resident virus infects COM and EXE files (Any file with the name SCAN is safe). Infection takes place on any of these commands Open or Exec or Rename, or Change File Mode. The virus uses the standard EXE/COM infection techniques.

Sticky identifies itself in MBS, memory , EXE files and COM files. The MBS' ID occupies 18 bytes from offset 1Ah. The memory's ID is a value of 1234h from register. The COM's ID is the 4the byte to be equal the second byte - 1. The EXE files' ID is to set the Initial IP to 1.

Sticky does not any payload. No attempt has been make to hide the virus infection in the directory or file.

Warning: Sticky infects on Open command. Any scanner that can not detect the virus in memory will spread the virus everywhere. Using an infected PC to scan a server means disaster. When any executable network files are executed, then MBS and Workstations on the network will be infected.

The recommended method for MBS disinfection is using a clean boot to start and FDISK/MBR command. Replace infected file by a clean backup copy on clean boot.

Name: Stimp		
Aliases: Stimp	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Stinkfoot		
Aliases: Stinkfoot, Paul Ducklin, Ducklin	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Overlays application, no increase adds either 1254 bytes or 1273 bytes	**See Also:**
Notes: written (poorly) in assembler, found in South Africa virus tries to adjust INT 24h (Critical Error Handler) to its own code, author wrote non-working INT 24h code. Any critical errors after the virus has run bring down the system. When run, current directory is examined for .COM files; 1st uninfected one over 512 bytes is hit; IF the target .COM is the first one in its directory, virus hits it regardless of its size. If it was too small, it will no longer run (will hang PC) 1 version adds 1254 bytes to files, says "StinkFoot has arrived on your PC !", displayed in Black on Black if infected file is executed with DOS time minutes=seconds 2nd version adds 1273 bytes, says "StinkFoot: '(Eat this Paul Ducklin)'" displayed if hours=minutes (Black on Black) (Paul Ducklin is a South African anti-viral program developer)		

Name: Stoned		
Aliases: Stoned, Marijuana, Hawaii,New Zealand, Australian, Hemp, San Diego, Smithsonian, Stoned-B, Stoned-C, Zapper (variant)	**Type:** Boot sector.	
Disk Location: Floppy disk boot sector.Hard disk boot sector.Hard disk partition table.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts boot sectorCorrupts the file linkages or the FAT.	**Size:** Overlays boot sector, no increase, 440 bytes	**See Also:** Michaelangelo
Notes: Spreads between boot sectors of both fixed and floppy disks. May overlay data. Sometimes displays message "Your PC is now Stoned!" when booted from floppy. Affects partition record on hard disk. No intentional damage is done. When Stoned and Michaelangelo both infect a disk, problems occur because they both try to hide the partition table in the same place. 'Your PC is now Stoned!.....LEGALISE MARIJUANA!' in the bootsector at offset 18Ah		

Name: Storm		
Aliases: Storm	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Storm (1172 and 1218)		

Name: Stupid.Sadam.Queit		
Aliases: Stupid.Sadam.Queit	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Stupid.Sadam.Queit.B		

Name: SUG		
Aliases: SUG	**Type:** Trojan.Encrypted/Stealth The virus actively hides.	
Disk Location: SUG.???	**Features:** Encrypted	
Damage: Erases a Floppy Disk	**Size:**	**See Also:**
Notes: This program is supposed to unprotect copy protected program disks protectedby Softguard Systems, Inc. It trashes the disk and displays: "This destruction constitutes a prima facie evidence of your violation. If you attempt to challenge Softguard Systems Inc..., you will be vigorously counter-sued for copyright infringement and theft of services." It encrypts the Gotcha message so no Trojan checker can scan for it.		

Name: Sunday		
Aliases: Sunday, Sunday-B, Sunday-C	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 163616441631uses INT 21 subfunction FF to check for prior infections	**See Also:** Jerusalem
Notes: Infects .OVL, .COM and .EXE files. It is a memory resident virus. It can affect system run-time operations. It appears to be a "Jerusalem" variant, with modifications at the source code level to make this a separate and distinct virus (i.e. not a mutation of Jerusalem). First discovered in Seattle, WA in November 1989. Three variants exist. FAT damage has been reported, but not confirmed. Each of the three variants adds a different amount of bytes to files, it is not yet known which size is for which variant. One variant only is damaging; it activates on Sundays and displays a message. The other two variants have a bug which stops this action, and do not cause FAT damage. Works well on LANs Activation on Sundays and displays message "Today is Sunday! Who do you work so hard? All work and no play make you a dull boy. C'mon let's go out and have fun!" then may cause FAT damage Find with standard detection/eradication packages FPROT 2.00, probably earlier versions, most commercial scanners.		

Name: Sundevil		
Aliases: Sundevil	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Suriv-01		
Aliases: Suriv-01, April-1-COM, April 1st, Suriv A, sURIV 1.01	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 897	**See Also:**
Notes: Spreads between COM files. On April 1st, 1988, writes the message: "APRIL 1ST HA HA HA HA YOU HAVE A VIRUS" and hangs the system. After that, simply writes a message every time any program is run. If day is greater than 1st April, only "YOU HAVE A VIRUS !!!" is displayed. Typical text in Virus body (readable with HexDump-utilities): "sURIV 1.01"		

Name: Suriv-03		
Aliases: Suriv-03, Suriv03, Suriv 3.00,Suriv 3.00, Suriv B, Jerusalem (B), Israeli #3	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1813 bytes increase in length of .COM files1808-1823 bytes increase in length of .EXE files	**See Also:**
Notes: The system is infected if function E0h of INT 21h returns value 0300h in the AX-register. .Com files: program length increases by 1813; files are infected only once; COMMAND.COM is not infected. .EXE files: program length increases by 1808 - 1823 bytes, and no identification is used; therefore, .EXE files can be infected more than once. Programs are infected at load time. 30 seconds after the 1st infected program was run, the virus scrolls up 2 Lines in a small window of the screen (left corner 5,5; right corner 16,16). The virus slows down the system by about 10 %. Suriv 3.00 compares the system-date with "Friday 13th", but is not able to recognize "Friday 13th", because of a "bug"; if it correctly recognized this date, it would delete any program started on "Friday 13th". Increase in the length of .EXE files. Lines scrolling in a small window. General slowdown of a machine. Typical texts in Virus body (readable with HexDump facilities): "sURIV 3.00"		

Name: SVC 6.0		
Aliases: SVC 6.0	**Type:** Program.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:** Starship
Notes: Russian origin virus, infects device drivers (see also Starship virus) v6-151: At least one anti-virus program can detect and remove SVC (1689.B, 1689.C, and 3103.D)		

Name: Swap Boot		
Aliases: Swap Boot, Falling Letters Boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sector	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: The virus overwrites the boot with a loader that loade the rest of the virus stored near the end of track 39. The virus makes letters fall down the screen.		

Name: Sybille		
Aliases: Sybille	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Sylvia V2.1		
Aliases: Sylvia V2.1,Holland Girl	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 13321321	**See Also:**

Notes: The virus infects only COM-files with less than 30 KB; it does not infect COMMAND.COM, IBMBIO.COM, IBMDOS.COM. 1301 bytes of the virus-code are written in front of and 31 bytes are written behind the original code; files are only infected once, because the virus checks the existence of its signature (808h) at the beginning of the file.
When an infected file is started, the virus tries to infect 5 COM-files on default drive.
The virus displays the following message : "FUCK YOU LAMER !!!! (CRLF) system halted..." and stops system by jumping into an endless loop. The message is encoded in the program.
In this version (V2.1), the message typical for original Sylvia virus ("This program is infected by a HARMLESS ... ") is NOT displayed.
After being activated, the virus checks itself by creating a check-sum of the first 144 words. When the check-sum is incorrect (# 46A3h) the damaging part of the virus is activated.
"FUCK YOU LAMER !!!! (CRLF) system halted", displayed on screen. Typical texts in Virus body (readable with Hexdump-facilities) :

1. "39 38 39 38 4F 45 4F 52 61 59 1E 56 5D 5A 52 61 62" (encoded text)
2. 'Text-Virus V2.1'
3. 'Sylvia Verkade'

808h at beginning of file.

Name: Syslock		
Aliases: Syslock, Macrosoft	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** EncryptedDirect acting.	
Damage: Corrupts a program or overlay files.Corrupts a data file.	**Size:** 3550-3560 bytes are appended on a paragraph boundary	**See Also:**

Notes: Spreads between .COM and .EXE files. It scans through data on the hard disk, changing the string "Microsoft" (in any mixture of upper and lower case) to "MACROSOFT". If the environment variable "SYSLOCK=@" is set, the virus will not infect. A variant of Advent. Microsoft changes to MACROSOFT
v6-151: At least one anti-virus program can detect and remove Syslock.C and Syslock.D.

Name: Tack		
Aliases: Tack	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:** 411477	**See Also:**

Notes: v6-151: Overwrites/destroys infected files.

Name: Tai-Pan		
Aliases: Tai-Pan, Whisper	**Type:** Program.	
Disk Location: EXE application.Only .EXE apps less than 64K long.	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 438	**See Also:**

Notes: Tai-Pan was discovered in Sweden in the summer of 1994, and has spread to Europe, USA, New Zealand, and Canada .
Tai-Pan is a simple virus.
It is memory resident and infects all executed .EXE files that are less than 64 KB in length. Infected files grow by 438 bytes.
The virus is not destructive, but makes infected machines unstable.

Text contained in the file: `[Whisper presenterar Tai-Pan]'.

Name: Taiwan		
Aliases: Taiwan, Taiwan 2, Taiwan-B, Taiwan 3, Taiwan 4, 2576	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Taiwan (708.B, 743.B and 752.B		

Name: Telefonica		
Aliases: Telefonica, Spanish Telecom, Telecom Boot, Anti-Tel, A-Tel, Campanja, Campana, (see also Antitelefonica), Kampana	**Type:** Boot sector.	
Disk Location: COM application.EXE application.Floppy disk boot sector.Hard disk boot sector.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorCorrupts the file linkages or the FAT.Attempts to format the disk.	**Size:**	**See Also:**
Notes: The Telefonica COM/EXE file infector can contain the Campana boot sector virus. Campana only affects the bootblock of floppies and partition table of hard disks. To eradicate from HD boot from clean floppy, and with DOS 5, type FDISK /MBR to rebuild the partition table. Or try most anti-viral utilities, they should clean it. Campana may try to format the hard disk after 400 reboots. If the virus has trashed the disk, probably can't recover the Antitelefonica variant is a multi-partite virus (see record of that virus for more info)		

Name: Terror		
Aliases: Terror, Dark Lord	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: a new version was found recently in Bulgaria in the wild, does not seem to work properly, mentioned in virus-l, v4-224		

Name: Testvirus-B		
Aliases: Testvirus-B	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Testvirus-b (B and C).		

Name: The Basic Virus		
Aliases: The Basic Virus, 5120, V Basic Virus	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:** 5120-5135 bytes change in length. Code added at a paragraph boundary.	**See Also:**
Notes: The virus infects programs at run time (it is not memory resident) by searching through the directories recursively starting on paths "C:\", "F:\" as well as the current drive. All .EXE and .COM files it can find are infected. EXE files will be infected if the length as reported by DOS is less that the file length as reported by the EXE header plus one page. COM files will be infected if the file length is less than 60400 bytes. The virus will infect any time it is executed after the 6th of July 1989. However, an infected file will infect before this date, if it has already been executed once. On any date after the 1st of June, 1992, any infected file will terminate with the message "Access denied" (this comes from the virus, not from DOS). After 1/1/92, executed programs terminate with an "Access denied" error. The following texts are contained in the virus: "BASRUN", "BRUN", "IBMBIO.COM", "IBMDOS.COM", "COMMAND.COM", "Access denied"		

Name: Thirty-three		
Aliases: Thirty-three, 33	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Tic		
Aliases: Tic	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Tic.97.		

Name: Timid		
Aliases: Timid	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Timid.302		

Name: Tiny 163		
Aliases: Tiny 163, V 163, V-163	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage:	**Size:** 163 Added to .COM files. that start with a JMP instruction	**See Also:**
Notes: When an infected file is executed, the virus attempts to infect other .COM files in the local directory. Files increase in length. v6-141: " ...a Tiny variant can't be loaded elsewhere and be still active. All viruses in the Tiny family (I mean the Bulgarian ones; not Danish_Tiny, Tiny-DI, Tiny-GM, or whatever - I have not checked them) must install themselves at a particular address. If somebody rewrites the virus to use a completely different memory allocation strategy - well then it will be a sufficiently different virus and will belong to another family. :-)..."		

Name: Tiny virus		
Aliases: Tiny virus, Tiny 134, Tiny 138, Tiny 143, Tiny 154, Tiny 156, Tiny 158, Tiny 159, Tiny 160, Tiny 169, Tiny 198, Tiny 133	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** tiny
Notes: see tiny		

Name: TIRED		
Aliases: TIRED	**Type:** Trojan.	
Disk Location: TIRED.???	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Another scramble the FAT trojan by Dorn W. Stickel.		

Name: Tomato		
Aliases: Tomato	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Toothless		
Aliases: Toothless, W13, W13-A, W13-B	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 534, 507	**See Also:**
Notes: Infects .COM files. Infected programs are first padded so their length becomes a multiple of 512 bytes, and then the 637 bytes of virus code is added to the end. It then intercepts any disk writes and changes them into disk reads.		

Name: TOPDOS		
Aliases: TOPDOS	**Type:** Trojan.	
Disk Location: TOPDOS.???	**Features:**	
Damage: Attempts to format the disk.	**Size:**	**See Also:**
Notes: This is a simple high level [hard] disk formatter.		

Name: Totoro Dragon		
Aliases: Totoro Dragon, Totoro Cat	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1540 bytes	**See Also:**

Notes: from virus-l, v6-109:
It is a resident .COM, and .EXE infector, and is 1540 bytes in length. I don't believe it is in the wild, but you never know.

The text below is contained in the virus

Totoro Dragon
Hello! I am TOTORO CAT
Written by Y.T.J.C.T
in Ping Tung. TAIWAN
Don't Worry, be Happy
$YTIT

Totoro Dragon is neither a stealth or encrypted virus. It has an odd method of infecting .COM files. the virus is placed at the beginning of the file, and adds four bytes of text at the end of the file YTIT. In .EXE files, the virus is appended to the end, and again, YTIT is placed at the end of the file Adding YTIT to the end of the infected files is how that Totoro Dragon marks files as infected.

Name: TPE		
Aliases: TPE, Trident Polymorphic Engine	**Type:** Virus Authoring Package (VAP).	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**

Notes: all TPE-based viruses contain the string "[MK / Trident]"
McAfee v105 says TPE is TridenT.

Name: TPWORM		
Aliases: TPWORM	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**

Notes: A companion virus (v4-121)

Name: Traceback		
Aliases: Traceback, 3066, 3066-B, 3066-B2, Traceback-B, Traceback-B2	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 3066	**See Also:**
Notes: Spreads between COM and EXE fles. Based on a rather complicated set of criteria, it will sometimes cause the text displayed on the screen to fall to the bottom, and then rise back up. One hour after system infection, the characters will fall down the screen. After 1 minute, screen is automaticly restored. During damage, INT 09h will be hooked. Characters typed during damage will move "fallen-down" characters back to their start position. Damage repeats every hour. Typical text in Virus body (readable with hex-dump-utilities): 1. "VG1" in the data area of the virus 2. "VG1" is found at offset of near-jmp- displacement if program is a .COM file. 3. The complete name of the file, which infected the currently loaded file, is in the code. 4. Search the last 16 bytes of a .COM or .EXE files for the hex-string: 58,2B,C6,03,C7,06,50,F3,A4,CB,90,50,E8,E2,03, 8B		

Name: Traceback II		
Aliases: Traceback II, 2930, 2930-B, Traceback II-B	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 2930	**See Also:**
Notes: This appears to be an earlier version of Traceback. Spreads between .COM and .EXE files. Based on a rather complicated set of criteria, it will sometimes cause the text displayed on the screen to fall to the bottom, and then rise back up. Text falls down the screen.		

Name: Trackswap		
Aliases: Trackswap, VB Trackswap	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Swaps tracks from the front with end of floppy tracks, making it real difficult to disinfect Not seen in wild by DDI		

Name: Traveler Jack		
Aliases: Traveler Jack	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Traveler Jack (854, 979, 980 and 982)		

Name: Tremor		
Aliases: Tremor, Tremor2	**Type:** Memory resident; TSR.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: Polymorphic, stealth, tunneling, direct attacks some anti-virus software big in Europe, mainly Germany Disables VSAFE from DOS 6.0 (the resident antivirus program)(v6-084) Find with: FPROT 2.08 TBCLEAN, ANTISER, Vi-Spi, SCAN 9.18V106 McAfee calls it Tremor2 in scan 9.18V106 Can possibly, in some cases, manually get rid of the virus by saving files a different way to allow the virus to uninfect the files. If you have the virus, examine the virus-l digest v6 issue 141 for a message that might work.		

Name: TridenT		
Aliases: TridenT	**Type:** Program.	
Disk Location: EXE application.	**Features:** EncryptedMemory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: it not related to Trident/TPE		

Name: Trigger		
Aliases: Trigger	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Polymorphic	
Damage: Corrupts a program or overlay files.	**Size:** files grow by 2493-2653 bytes	**See Also:** MtE
Notes: Trigger infects .COM and .EXE files from 2 bytes - 29696 bytes. The researcher's largest bait file was 29K 29696 bytes. Trigger has the following text in the first generation (Trigger by Dark Angel of Phalcon/Skism Utilising Dark Angel's Multiple Encryptor (DAME)). No text is readable in the second generation and beyond. Trigger is polymorphic, but not stealth. On the test machine, the files grew by 2493 bytes - 2653 bytes Trigger appends the virus to the end of the host files.		

Name: Trivial		
Aliases: Trivial	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Versions include: 26.B, 27, 28, 29, 30.D, 30.E, 40.D, 40.E, 40.F, 42.C, 42.D, 43, 44.D, 45.D,and 102 v6-151: Overwrites/destroys infected files.		

Name: Trivial-64		
Aliases: Trivial-64, Trident	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: contains the internal string "Trident"		

Name: Troi		
Aliases: Troi, Best Wishes, Best Wish (may be wrong), Troi Two	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** Adds 322-324 bytes to infected .com files	**See Also:**
Notes: Hinders execution of some programs. Virus code is located at the end of the orig. .com file and is jmp - ed toas a FAR procedure. Attempt to infect a file on a write prot. disk will produce "Abort, retry, fail?" message SCAN 86B says its the Best Wishes virus, but this may be wrong. Programs monitoring disk activity will trap the infection requests. Easy to detect as it changes the times and dates for infected files to outrageous times and dates. Approximately fifty-six YEARS are added to the date. HEX search string: 2AC0CF9C80FCFC75, also scan for string "The Troi Virus" FPROT 2.03a		

Name: TSRMAP		
Aliases: TSRMAP	**Type:** Trojan.	
Disk Location: TSRMAP.???	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: TSRMAP *TROJAN* This program does what it's supposed to do: give a map outlining the location (in RAM) of all TSR programs, but it also erases the boot sector of drive "C:".		

Name: Twin-351		
Aliases: Twin-351	**Type:** Companion program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 351 bytes	**See Also:**
Notes: Unlike the other two companion viruses (AIDS II and TPWORM) it stays resident in memory, intercepting the Findfirst/FindNext calls. As the files containing the virus are also marked as "hidden", the virus is able to hide quite efficiently, unless a program reads the directory directly. Suspected not found outside of Norway		

Name: Typo		
Aliases: Typo, Type Boot	**Type:** Boot sector.	
Disk Location: Floppy disk boot sectors.Hard disk boot sectors.	**Features:** Memory resident; TSR.	
Damage: Corrupts boot sectorInterferes with a running application.	**Size:** Overlays boot sector, no increase	**See Also:**
Notes: Infects floppy and hard disk boot sectors. Infects data disks as well as system disks. Attempting to boot with an infected data disk in the drive loads the virus then asks for a system disk. Every 50 printed characters, the virus inserts a typo. Typos in printed output. 80286 and 80386 machines hang when booted with an infected disk. You can detect infected diskettes by running Chkdsk . If you get 1k of bad sectors, that's a good sign of Typo (or Italian virus), as FORMAT marks an entire track (5k on a 360k diskette) as bad if it finds a defect. Treatment consists of simply copying all the files off an infected diskette (using "COPY *.*"; do not use Diskcopy or any image copier), and reformatting the diskette		

Name: Typo		
Aliases: Typo, Fumble, Typo COM, 867, Mistake	**Type:** Program.	
Disk Location: COM application.COMMAND.COM.	**Features:** Direct acting.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 867	**See Also:**
Notes: Infects .COM files. The virus replaces the keyboard handler, and if it is in place, it occasionally replaces the key that is typed, with the key immediately to the right. The fumble only activates if you type at better than six characters per second (approximately 60 wpm). If you type at that speed, after not using the keyboard for five seconds, you get a fumble. Typed characters are not what you pressed. v6-151: At least one anti-virus program can detect and remove Fumble.E		

Name: ULTIMATE		
Aliases: ULTIMATE	**Type:** Trojan.	
Disk Location: ULTIMATE.ARCULTIMATE.EXE	**Features:**	
Damage: Corrupts the file linkages or the FAT.	**Size:** 3090 size of ULTIMATE.EXE2432 Size of ULTIMATE.ARC	**See Also:**
Notes: Another FAT eater		

Name: Ultimate Weapon		
Aliases: Ultimate Weapon, Smulders's virus, Criminal	**Type:** Program.	
Disk Location: COM application.EXE application.COMMAND.COM.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: A Dutch virus, activated after Jan 1, 1992, after boot a message is displayed (sic): The Ultimate Weapon has arrived, please contact the nearest police station to tell about the illegal copying of you The system will hang, after boot from floppy in A: all files and directories in the root and the next directory-level renamed to CRIMINAL.001, CRIMINAL.002 etc See also Criminal virus signature given in virus-l v5-011: MF00EVKUR		

Name: Ultimatum		
Aliases: Ultimatum	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Sometimes reported by Fprot 2.09b or earlier versions as a false positive...has been fixed in later versions of Fprot.		

Name: Unexe		
Aliases: Unexe	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Uruguay		
Aliases: Uruguay	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: from Uraguay, has been around since Dec 1992		

Name: Uruk Hai		
Aliases: Uruk Hai	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Uruk Hai.427.		

Name: USSR		
Aliases: USSR, USSR 516, USSR 600, USSR 707, USSR 711, USSR 948, USSR 1049, USSR 1689, USSR 2144, USSR 1594	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different(USSR-1594 only alters one byte)	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Ussr-707.B		

Name: V-299		
Aliases: V-299, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 299	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V-345		
Aliases: V-345, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 345	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus contains an advertisement for Amstrad computers. The program prints "Program sick error:Call doctor or buy PIXEL for cure description" with a 50-50 chance after the 5th infection. The virus contains the string "Program sick error:Call doctor or buy PIXEL for cure description". The string "IV" is at offset 3 in the COM file.		

Name: V08-15		
Aliases: V08-15	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage:	**Size:** 1322 -1337 virus is placed on even paragraphs	**See Also:**

Notes: A .COM and .EXE file infector. After the 11th of November 1990 the virus will intercept INT 09 and count the keystrokes. If the number of keystrokes reaches 3000 the virus will display the message "CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR". and halt the system. Counting starts as soon as the first infected file is started.
CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR. printed on screen. Infected files contain the readable string:
'CRITICAL ERROR 08/15: TOO MANY FINGERS ON KEYBOARD ERROR.'
EXE-type files are marked infected by 4D54h at offset 12h (that is the EXE header checksum).
COM-type files are marked by the same 16bit value but at offset 3 in file (that is 103h when loaded). Boot from a clean disk and delete infected files.

Name: V1701New		
Aliases: V1701New, V1701New-B, Evil, Evil-B, P1, Phoenix related	**Type:** Program.Encrypted/Stealth The virus actively hides.	
Disk Location: COM application.COMMAND.COM	**Features:** Memory resident; TSR above TOM.EncryptedPolymorphic	
Damage:	**Size:** 1701 All .COM files but COMMAND.COMIt overlays part of COMMAND.COMMulti ple infections are possible.Polymorphic: each infection different	**See Also:**

Notes: The V1701-New virus is of Bulgarian origin, a variant of Phoenix. The V1701-New virus is a memory resident, generic infector of .COM files, and will infect COMMAND.COM. V1701-New infects COMMAND.COM by overwriting part of the binary zero portion of the program, and changing the program's header information. COMMAND.COM will not change in file length. V1701-New is not able to recognize when it has previously infected a file, so it may reinfect .COM files several times. Each infection of a .COM file will result in another 1,701 bytes of viral code being appended to the file. Systems infected with the V1701-New virus will experience problems with executing CHKDSK.COM. Attempts to execute this program with V1701-New memory resident will result in a warm reboot of the system occurring, however the memory resident version of V1701-New will not survive the reboot. The V1701-New Virus employs a complex encryption mechanism, and virus scanners which are only able to look for simple hex strings will not be able to detect it. There is no simple hex string in this virus that is common to all infected samples.
Also see: PhoenixD, Phoenix
A warmboot occurs when CHKDSK.COM is run. ViruScan V66+ Scan/D, or delete infected files

Name: V2P2		
Aliases: V2P2	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: V2P6		
Aliases: V2P6, Vienna Variant, V2P6 Trash, V2P6Z, Adolph\	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: A polymorphic virus, the decryption routine and infection length vary lots, so its hard to locate all infected files. Otherwise, it is a vienna-related virus, non-resident, and infects only COM files in the current directory and in the directories listed in the PATH. VIRx has reported some false positives for this virus, in older versions of mem.com, popdrop.com, and HP.com. Virx21.zip should have fixed these false positives: reported in virus-l, v5-065 MS-DOS 6's antivirus routine detects some, but not all infections by V2P6.		

Name: Vacsina		
Aliases: Vacsina, TP04VIR, TP05VIR, TP06VIR, TP16VIR, TP23VIR, TP24VIR, TP25VIR	**Type:** Program.	
Disk Location: COM application.EXE application.Program overlay files.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1206 - 1221 Added to a .COM file length mod 16 equals 0132+ Added to .EXE file then like a com file.	**See Also:** Yankee Doodle
Notes: It infects .COM and .EXE files when they are loaded, old versions of the virus will be replaced by newer ones. System beep when running a program. The string 'VACSINA' in the virus code the last 4 bytes of an infected file show F4 7A 05 00 v6-151: At least one anti-virus program can detect and remove Vacsina (634,TP.5.B and TP.16.B)		

Name: Vbasic		
Aliases: Vbasic	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Vbasic.D.		

Name: Vcomm		
Aliases: Vcomm, 637	**Type:** Program.	
Disk Location: EXE application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 637	**See Also:**
Notes:		

Name: VDIR		
Aliases: VDIR	**Type:** Trojan.	
Disk Location: VDIR.???	**Features:**	
Damage: Attempts to erase all mounted disks.	**Size:**	**See Also:**
Notes: This is a disk killer that Jerry Pournelle wrote about in BYTE Magazine.		

Name: VFSI		
Aliases: VFSI, 437	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove VFSI.B		

Name: VHP		
Aliases: VHP, VHP-348, VHP-353, VHP-367, VHP-435, Faggot	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage:	**Size:**	**See Also:**
Notes: File infector, Faggot is somewhat of a virus/trojan, if its the first infection, it trashes the hard disk, but if it's not the first infection, it just sits there. May be related to VHP. It is probably a hack on the Vienna, but very poorly written.		

Name: Vienna		
Aliases: Vienna, 648, Lisbon, Vienna-B, Austrian, Dos-62, Unesco, The 648 Virus, The One-in-Eight Virus, 62-B, DOS-68, Vien6, Vienna-B645, 648-B, Choinka, W-13, Abacus, Bush, IWG	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.Deletes or moves files.	**Size:** 648	**See Also:**
Notes: The virus infects one .COM file every time it is run. 7/8 of the time it infects the .COM file and 1/8 of the time it inserts a jump to the BIOS initialitation routines that reboot the machine. To mark a file as infected, the virus sets the seconds field of the timestamp to 62 which most utilities (including DIR) skip. Damaged files, file lengths increase. The second-entry of the time stamp of an infected file is set to 62 dec.		

Name: Vienna 348		
Aliases: Vienna 348	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.Interferes with a running application.	**Size:** 348	**See Also:**
Notes: The time stampof an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the filesize<10 or filesize>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 7) <> 0 ELSE damaged! INT 24h diverted to own error-handler only during virus-runtime to suppress error-messages send out by DOS. A selected .COM-file is damaged permanently: Overwriting the first five bytes with a far jump to the HD-low-level-format- routine (XT only). The virus ignores READ-ONLY and HIDDEN attributes; A branch to the low level format routine on an XT when a program is run. Bytes found in virus = EAh,06h,00h,00h,C8h; text found: "*.COM",00h,"PATH=". Seconds time stamp changed to 62		

Name: Vienna 353		
Aliases: Vienna 353, Vienna 367, Vienna 435, Vienna 623, Vienna 627	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 353, 367, 435, 623, 627	**See Also:**
Notes: The time stampof an infected file is changed: the seconds are set to 62 (= 2 * 1Fh). When infected file is executed, .COM-files in the current directory as well as in the directories in the DOS-PATH are extended by appending the viral code; no infection if the filesize<10 or filesize>64000 bytes. A selected .COM-file is infected by "random" IF (system seconds AND 7) <> 0 ELSE damaged! INT 24h diverted to own error-handler only during virus-runtime to suppress error-messages send out by DOS. A selected .COM-file is damaged permanently: Overwriting the first five bytes with a far jump to the HD-low-level-format- routine (XT only). The virus ignores READ-ONLY and HIDDEN attributes; Bytes found in virus = EAh,06h,00h,00h,C8h; text found: "*.COM",00h,"PATH=". The time stamp of an infected file changes to 62		

Name: Viki		
Aliases: Viki, V-277, Amstrad	**Type:** Program.	
Disk Location: COM application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:** 277	**See Also:**
Notes: Adds code to front of any .COM file in the current directory. The virus simulates a RAM parity error. The program terminates with a simulated RAM parity error with a 50-50 chance after the 5th infection. The string "UM" at offset 3 in the COM file		

Name: Virus 101		
Aliases: Virus 101	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Virus Creation Lab		
Aliases: Virus Creation Lab, VCL, Anti-Gif, ByeBye, Earthquake, Paranoramia, Poisoning, VF93, VPT, Ziploc	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: The VCL is a program which creates viruses. It has a menuing routine which allows for easy creation of new viruses, using various selection criteria. It has been wide distributed on various bulletin boards. sometimes difficult, some antivirus products have only a 90% success rate in finding it. Data Physician Plus! claims over a 99% success rate Once found, it is easy to eradicate viruses created as all viruses are .exe and .com infectors DataPhusician Plus 4.0B has some false positives with VCL. The problem is corrected in version 4.0C. v6-151: VCL.527 Overwrites/destroys infected files. v6-151: At least one anti-virus program can detect and remove VCL (506, 507, 604, 951, Anti-Gif, ByeBye, Earthquake, Paranoramia, Poisoning, VF93, VPT and Ziploc)		

Name: Virus-90		
Aliases: Virus-90	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 857	**See Also:**
Notes:		

Name: Viruz		
Aliases: Viruz	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Vlad the Inhaler		
Aliases: Vlad the Inhaler	**Type:** Not a virus/worm/other destructive procedure	
Disk Location:	**Features:**	
Damage: Does no damage, doesn't affect any part of machine	**Size:**	**See Also:**
Notes: NOT A VIRUS! This phrase was a false alert, a task titled "Vlad the Inhaler" shows up in the file NWRES.DLL which is part of the Norton Desktop program. Occasionally it appears to show up when upgrading to Windows 3.1. It is included here in case anyone sees it and thinks it may be a destructive piece of code.		

Name: Voice Master		
Aliases: Voice Master	**Type:** Trojan.	
Disk Location: Voice Master	**Features:**	
Damage: Corrupts boot sectorCorrupts the file linkages or the FAT.	**Size:**	**See Also:**
Notes: Since the IBM PC speaker could make a very poor microphone but the system electronics is designed only for sound output, the programs claims (see below) could be evidence of malicious purpose. Found on a BBS in Virginia, USA Will attempt to overwrite the Boot record, both FATs and a portion of the root dir on all disks using Interrupt 26. At this time not known if it will occur on each activation or if their is a discriminator in use (disassembly is 54 pages long)		

Name: Vootie		
Aliases: Vootie	**Type:** Program.	
Disk Location: EXE application.COM application.	**Features:** Direct acting.	
Damage:	**Size:** 66 bytes	**See Also:**
Notes: Overwrites both .EXE and .COM files, all files in the current directory, displays garbage when the file is run.		

Name: Voronezh		
Aliases: Voronezh, Voronezh B, Voronezh-1600	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Direct acting.	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Voronezh-1600 places a Far CALL to its body at the EXE file's entry point This virus does not change the file entry point, as does Leapfrog and Brainy		

Name: Warpcom-II		
Aliases: Warpcom-II, CD-IT.ZIP, Chinon	**Type:** Trojan.	install.com in CD-IT.ZIP archive
Disk Location: Trojan program.	**Features:** Direct acting.	
Damage: Overwrites first 256 logical sectors of drive D with garbage.Corrupts command.com	**Size:** Overlays application, no increase	**See Also:**

Notes: Reported by Chinon in a press release.
> >TORRANCE, CALIFORNIA, U.S.A., 1994 APR 29 (NB) -- A new "Trojan
> >Horse" computer virus is on the Internet and is labeled with the
> >name of the fourth largest manufacturer of compact disc read-only
> >memory (CD-ROM) drives. Chinon America, Incorporated, the company
> >whose name has been improperly used on the rogue program, is
> >warning IBM and compatible personal computer (PC) users to beware
> >of the program known as "CD-IT.ZIP."
> >
> >A Chinon CD-ROM drive user brought the program to the company's
> >attention after downloading it from a Baltimore, Maryland
> >Fidonet server. One of the clues that the virus, masquerading as
> >a utility program, wasn't on the up-and-up was that it purports "to
> >enable read/write to your CD-ROM drive," a physically impossible
> >task.

> >CD-IT is listed as authored by Joseph S. Shiner, couriered
> >by HDA, and copyrighted by Chinon Products. Chinon America told
> >Newsbytes it has no division by that name. Other clues were
> >obscenities in the documentation as well as a line indicating
> >that HDA stands for Haven't Decided a Name Yet.
> >
> >David Cole, director of research and development for Chinon, told
> >Newsbytes that the company knows of no one who has actually been
> >infected by the program. Cole said the virus isn't particularly
> >clever or dynamic, but none of the virus software the company
> >tried was able to eradicate the rogue program. Chinon officials
> >declined to comment on what antivirus software programs were
> >used.
> >
> >If CD-IT is actually run, it causes the computer to lock up,
> >forcing a reboot, and then stays in memory, corrupting critical
> >system files on the hard disk. Nothing but a high-level reformat
> >of the hard disk drive will eradicate the virus at this point, a
> >move that sacrifices all data on the drive. It will also corrupt
> >any network volumes available.
> >
> >"We felt that it was our responsibility as a member of the
> >computing community to alert Internet users of this dangerous
> >virus that is being distributed with our name on it. Even though
> >we have nothing to do with the virus is it particularly
> >disturbing for us to think that many of our loyal customers could
> >be duped into believing that the software is ours," Cole
> >explained.
> >Chinon is encouraging anyone who might have information that
> >could lead to the arrest and prosecution of the parties
> >responsible for CD-IT to call the company at 310-533-0274.. In
> >addition, the company has notified the major distributors of
> >virus protection software, such as Symantec and McAfee Associates,
> >so they may update their programs to detect and eradicate CD-IT.
> >
> >(Linda Rohrbough/19940429/Press Contact: Rolland Going, The
> >Terpin Group for Chinon, tel 310-798-7875, fax 310-798-7825;
> >Public Contact: Chinon, CD-IT Information, 310-533-0274)
> >

The virus is actually the Warpcom-2 Trojan in a new archive. The Trojan overwrites toe copy of command.com with a short program that overwrites the D drive followed by a lot of hex FFs to fill out the file. The program that overwrites the D drive writes garbage to the first 256 sectors, though it does not seem to always work.

```
mov    aL,03        AL contains the disk number, 3=D
mov   cx,00ffh     CX contains the number of sectors to write
mov   dx,0000h  DX contains the first sector to write.
int      26h           Interrupt 26h, Absolute disk write
sbb    bh,bh         trash.
```

the interrupt also requires DS:BX to have value, as a pointer to the buffer to write to disk. Since these are not set in the program, you get whatever they happened to contain. I tried running this on a DOS 5 machine, and it did not seem to work. Int 26 is marked as superceeded in the dos programmers reference, so it is possible that it has been deleted.

Name: Warrier		
Aliases: Warrier, Brainy	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Corrupts a program or overlay files.	**Size:** 1531	**See Also:**
Notes: Brainy related to "Warrier" (not "Warrior"), mentioned virus-l, v4-224 Warrier may be broken, as virus-l writer was not able to infect anything, but Brainy may work OK. It may insert itself into the middle of a .COM program, without changing the beginning of the file, a trick which is only used by few other viruses (Leapfrog, and Voronezh-1600)		

Name: Westwood		
Aliases: Westwood	**Type:** Program.	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:** Jerusalem
Notes: v6-151: At least one anti-virus program can detect and remove Westwood.B.		

Name: Whale		
Aliases: Whale, Mother Fish, Z The Whale	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes:		

Name: Wilbur		
Aliases: Wilbur	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Wilbur (B and D).		

Name: Wildy		
Aliases: Wildy	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Willow		
Aliases: Willow	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Willow.2013.		

Name: WINSTART		
Aliases: WINSTART	**Type:** Companion program.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage: No damage, only replicates.	**Size:** 297 bytes long, BAT file	**See Also:**

Notes:
The following notes are extracted from VB, June 1995:

WINSTART is memory resident, BAT file infector.The installation routine is similar to BATMAN (first memory resident BAT virus). The body of the virus is found in a file named WINSTART.BAT which 297 bytes long. The file contains the 4 lines of text, followed by binary data. These 4 lines give a good insight to the method of operation, and they are:

```
@ECHO    OFF
:s%r#
 COPY %0.BAT    C: \ Q.COM> NUL
C : \ Q
```

When WINSTART.BAT file is executed, the virus disables echoing. Then copies itself into Q.COM that is placed at root directory of the derive C:, and Q.COM is executed. After the text, the first byte of the binary data is 1Ah, which is 'end-of-file'. Thus, the Q.COM is ended and control is returned to BAT.
The Q.COM is a copy of WINSTART.BAT so it contains identical data, but they are interpreted as Intel instruction codes. So the line ' :s%r# ' will insure that control is passed to binary part of the virus. The binary will install the memory resident portion of WINSTART into system memory. The virus hooks Int 2Fh and uses the Int 2Fh routines for its installation in high memory. Finally, C: \ Q.COM is renamed to C: \ WINSTART.BAT , the C: \ Q.COM is deltated, then the C: \ WINSTART.BAT is given the attributes of read only and its terminated.

The memory resident copy will infect floppy disk. The manner of infection is similar to above(i.e. Int 2Fh handler is employed). Infection takes place only when 2 conditions are met:
1) The current drive is A: or B:
2) The is more 50% full.
If it decides to go ahead and infect the floppy disk , then DOS error messages are suppressed via Int 24h.

The recommended method for disinfection is to delete WINSTART.BAT file.

Name: Wisconsin		
Aliases: Wisconsin, Death to Pascal	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Wisconsin.B.		

Name: Wolfman		
Aliases: Wolfman	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Wordswap 1485		
Aliases: Wordswap 1485, Wordswap 1504, Wordswap 1385, 1391	**Type:**	
Disk Location:	**Features:** Polymorphic	
Damage:	**Size:** Polymorphic: each infection different	**See Also:**
Notes: 1385 and 1391 won't work at all for one researcher		

Name: Wvar		
Aliases: Wvar	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Xph		
Aliases: Xph	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Xph (1029 and 1100).		

Name: Xtac		
Aliases: Xtac	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove this virus.		

Name: Xuxa		
Aliases: Xuxa, Surviv	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:** suriv 1
Notes: v6-129: reported to play music under the right circumstances. Most common antivirus utilities should disinfect it, though you would be much better off to delete any infected software and restore it from either the original disks or uninfected backups. Xuxz is a variant of the Surviv virus family v6-130: The author of the virus is a fan of Xuxa (Xuxa is soccer player Pele's ex-wife. She has a TV show for children in Brazil and in Argentina.) Xuxa virus is a Suriv 1 hack. It plays at 5 PM every day the theme song of Xuxa show, and stops at 6 PM. At that time is when the show was broadcasted here in Argentina.		

Name: Yankee Doodle		
Aliases: Yankee Doodle, Five O'Clock, TP33VIR, TP34VIR, TP38VIR, TP41VIR, TP42VIR, TP44VIR, TP45VIR, TP46VIR, Yankee Doodle 44, Enigma, Old Yankee	**Type:** Program.	
Disk Location: COM application.EXE application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1961162417552772 Yankee Doodle-B	**See Also:** vacsina
Notes: One day in about 8 at 5 pm it can play the "Yankee Doodle" tune This virus also uses hamming codes to check itself and repair itself if someone had modified it. TP44 virus: at 15 seconds before 5 pm it plays the Yankee Doodle tune Yankee Doodle coming from the computer's speakers. One of the easier viruses to disinfect, lots of softwar will do it. v6-151: At least one anti-virus program can detect and remove Yankee Doodle.Login.2967.		

Name: YB-1		
Aliases: YB-1	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:** 426 bytes	**See Also:**
Notes: not in wild		

Name: Youth		
Aliases: Youth	**Type:** Program.	
Disk Location: COM application.	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-151: At least one anti-virus program can detect and remove Youth.640.B		

Name: Zero Bug		
Aliases: Zero Bug, Agiplan, 1536, Palette, ZBug	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage: Interferes with a running application.Corrupts a program or overlay files.	**Size:** 1536	**See Also:** Dark Avenger
Notes: Infects .COM files. All characters "0" (zero) will be exchanged with other characters. Exchange characters are 01h, 2Ah, 5Fh, 3Ch, 5Eh, 3Eh and 30h, in which case the attribute is set to back- ground color (i.e. the character is invisible). This routine uses about 10% of CPU-time (system is slowed down accordingly). The Dark Avenger may be a descendant of this virus. Typical text in Virus body (readable with HexDump-utilities): "ZE","COMSPEC=C:", "C:\COMMAND.COM". In infected .COM files the "seconds" field of the timestamp is changed to 62 sec (similar to GhostBalls original Vienna viruses).		

Name: ZeroHunt		
Aliases: ZeroHunt, Minnow	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: v6-084: preserves the file's date, time, attributes, AND file length. Will not be detected by the integrity checking of MSAV or VSafe.		

Name: ZigZag		
Aliases: ZigZag	**Type:** Program.	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: v6-151: Overwrites/destroys infected files.		

Name: Zombie		
Aliases: Zombie	**Type:** Program.	
Disk Location: COM application.	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: v6-127: doesn't infect COMMAND.COM, lame resident COM infector, his version has nothing to do with OS/2		

Windows Computer Virus Table

Name: Colors		
Aliases: Colors, Wordmacro Colors, macro	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage:	**Size:** Adds Macros to Word document files	**See Also:** WordMacro.Nuclear, Concept, DMV, FormatC

Notes: This virus uses the macro capability built into Microsoft Word (WordBasic) to add a virus to a Word document. Since this virus is written in the macro language, it is not platform specific, but will execute on any platform that runs Word 5 or later.

When you open an infected document, its auto open macro runs and installs an auto execute macro in your global macro file (normal.dot). Once that is done, the virus code is executed every time you startup Word. The virus code then writes copies of itself onto every document you save with Word.

When the virus triggers, it messes with your color tables.

When it is installed, it adds the following macros to your system:

AutoClose, AutoExec, AutoOpen, FileExit, FileNew, FileSave, FileSaveAs, Macros, ToolsMacro.

It replaces the menu items with the indicated macros, making it difficult to see that you have an infiction. The ToolsMacro command no longer lists the macros in a system. To see the files, choose the File Templates command and click the Organizer button to see the macros.

The Microsoft protection for the Concept virus does not work.
F-Prot 2.21 detects it.

The only protection y ou have is to disable all autoexecute macros.

Create a global macro named MyDisableAutoMacros.
Insert the following code in it:

```
Main
  DisableAutoMacros 1
End Sub
```

In the program group, select the word icon and choose the File Properties command. In the Command line box, change the command line to the following (leave the path pointing to your copy of winword):

c:\msoffice\winword\winword.exe /mMyDisableAutoMacros

Note that this will only disable automacros if you start word with the icon. If you start it by double clicking a document, the MyDisableAutoMacros macro does not run and you are not protected. You must hold down the Alt key when opening a document to disable all the automacros but AutoExecute. AutoExecute only runs when you start Word.

To clean a document once you have it open, use the Organizer to delete the macros from the file then save it. Organizer can also be used to delete any virus macros stored in the global macro file, normal.dot.

Name: DMV		
Aliases: DMV , Winword DMV	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** Adds Macros to Word document files	**See Also:** WordMacro.Nuclear , Concept, FormatC , Colors

Notes: This virus uses the macro capability built into Microsoft Word (WordBasic) to add a virus to a Word document. Since this virus is written in the macro language, it is not platform specific, but will execute on any platform that runs Word 5 or later.

When you open an infected document, its auto open macro runs and installs an AutoClose macro in your global macro file (normal.dot). Once that is done, the virus code is executed every time you close a document. The virus code then writes copies of itself onto every document you save with Word.

See the description of Colors for more information about accessing and protecting from this virus.

F-Prot 2.21 Detects it.

This macro does no damage. It is a demonstration only. It is not encrypted. It is easy to delete using the Tools Macros command.

Name: FormatC		
Aliases: FormatC, Winword FormatC, Format C, macro	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage: Attempts to format the disk.	**Size:** Adds Macros to Word document files	**See Also:** WordMacro.Nuclear , Concept, DMV , Colors

Notes: This virus uses the macro capability built into Microsoft Word (WordBasic) to add a virus to a Word document. Since this virus is written in the macro language, it is not platform specific, but will execute on any platform that runs Word 5 or later.

When you open an infected document, its auto open macro runs and installs an auto execute macro in your global macro file (normal.dot). Once that is done, the virus code is executed every time you startup Word. The virus code then writes copies of itself onto every document you save with Word.

The macro messes with your color tables.

See the description of Colors for more information about accessing and protecting from this virus.

F-Prot 2.21 does not detect it.

Name: Hot		
Aliases: Hot , Winword Hot, Wordmacro/Hot	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage: Deletes Word documents as they are opened.	**Size:** Adds Macros to Word document files	**See Also:** WordMacro.Nuclear , Concept, FormatC , Colors

Notes: Wordmacro/Hot is a word macro virus and is destructive. The Wordmacro/Hot virus attaches itself like the others, adding macros to documents and to the "normal.dot" global macro file. New documents are infected when they are saved. After about 14 days, the virus deletes the contents of any document as you open it and does a save which effectively wipes out the document. It is unlikely that you will be able to recover the contents of a file deleted in this way unless you have Make Backup turned on. Don't start opening the backup copies before cleaning the virus, because it will clear the contents of every document you open while it is active.

An infected document contains the following macros:

AutoOpen DrawBringInFrOut InsertPBreak ToolsRepaginat

When the virus infects the Word program, these macros are copied to "normal.dot" and renamed in the same order to:

StartOfDoc AutoOpen InsertPageBreak FileSave

The virus adds the item: "OLHot=nnnnn" to the winword.ini file where nnnnn is a date 14 days in the future. The virus uses this date to determine when it is going to trigger. The virus also checks for the existence of the file: "c:\dos\ega5.cpi" and does not infect a machine if the file exists. This was apparently a feature to protect the virus writer.

See the description of Colors for more information about accessing and protecting from this virus.

Name: WinVir14		
Aliases: WinVir14, Win14, Windows virus	**Type:** Windows virus	
Disk Location:	**Features:**	
Damage: no damage, doesn't affect any part of machine	**Size:**	**See Also:**
Notes: From an article in Network World, November 23, 1992 (see article text below) if an infected program is run from dos prompt, it doesn't infect. Only if run from in windows The string MK92 is found in the virus, not used as actual data. After infecting all other programs in the dir, it deletes itself from the host program so it seems that the user simply mis-double-clicked the file, and the user doesn't knwo a virus has attacked.		

Name: WinWord.Concept		
Aliases: WinWord.Concept , Word Prank Macro, Concept, macro	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage: No damage, only replicates.	**Size:** Adds Macros to Word document files	**See Also:** WordMacro.Nuclear , FormatC, Colors, dmv, Hot

Notes: This virus uses the macro capability built into Microsoft Word (WordBasic) to add a virus to a Word document. Since this virus is written in the macro language, it is not platform specific, but will execute on any platform that runs Word 5 or later.

When you open an infected document, its auto open macro runs and installs an auto execute macro in your global macro file (normal.dot). Once that is done, the virus code is executed every time you startup Word. The virus code then writes copies of itself onto every document you save with Word.

This is the first virus discovered of this type. It does nothing but replicate itslef. You can detect the virus the first time it executes, because a dialog box appears containing the single digit 1. After the first infection, you can detect an infection by looking for the following line in the WINWORD6.INI file in the WINDOWS directory.

WW6I= 1

Microsoft has made a disinfector available to detect and remove this virus from a system and from infected documents. The disinfector is a document named scan831.doc. It is available directly from Microsoft at :

The Microsoft World Wide Web site at http://www.microsoft.com/msoffice
MSN(tm), The Microsoft Network using go word: wordprankfix
The Word forums on other on-line services such as CompuServe® and America Online®
Customers can also get the tool by calling Microsoft's Product Support Services at 206-462-9673 for Word for Windows, and 206-635-7200 for Word for the Macintosh.

Name: WordMacro.Nuclear		
Aliases:	**Type:** Macro.	
Disk Location: WinWord documents	**Features:** Direct acting.	
Damage: Attempts to launch a program virus. Corrupts printed documents.	**Size:** Adds Macros to Word document files	**See Also:** WinWord.Concept

Notes: The WordMacro.Nuclear virus is similar in operation to the WinWord.Concept virus in how it infects files, but contains an additional payload. This virus contains a dropper for a DOS virus, as well as the document infector.
You can detect the virus by listing the macros installed in Word, using the Tools Macros command. In the Macro dialog box that appears, make sure that the Macros Available In: box is set to: All Active Templates. If all the macros in the following list are listed in the Macro Name list, you probably have the virus. If only some are there, you probably don't.

AutoExec
AutoOpen
DropSuriv
FileExit
FilePrint
FilePrintDefault
FileSaveAs
InsertPayload
Payload

You can also detect the virus when printing a document during the last 5 seconds of any minute. If you do, the following text appears at the top of the printed page.

"And finally I would like to say:"

"STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!"

Amiga
Computer Virus Table

Name: EM-Wurm		
Aliases: EM-Wurm, EuroMail Bomb	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: Apparently the virus edits startup-sequence to execute a program with the single letter name $A0. A file of this name is created in c:. Effects as described in the file: Damage routine: + Works only when devices [directories] EM or EUROMAIL or EUROSYS are available. + overwrites all Files in these directories with memory from MsgPort. + In damaged files: from $BC text 'clipboard.device'. + After that a pause of 3mins using dosdelay $259A + After pause damage routine is called again.		

Name: Saddam		
Aliases: Saddam	**Type:** Memory resident; TSR.	
Disk Location:	**Features:** Memory resident; TSR.	
Damage:	**Size:**	**See Also:**
Notes: Infects amiga's memory as soon as you insert an infected disk Disguises itself as the Disk-Validator, and sets about randomly altering all your vectors so that the disk becomes read-error happy. It eventually trashes your disk at some given trigger. A LINK virus VirusScan 5.32, Disaster Master 2		

Name: Smiley Cancer		
Aliases: Smiley Cancer	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts a program or overlay files.	**Size:**	**See Also:**
Notes: Not a bootblock-virus, but not a link-virus. It uses method similar to PC Dir II virus, because it changes some info in the file headers		

Atari
Computer Virus Table

Name:(Atari virus info)		
Aliases: (Atari virus info)	**Type:** Not a virus/worm/other destructive procedure	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: This record contains some Atari virus info in the Summary section, taken from virus-l, v5-187 About two dozens of them are described in the Atari ST section of the Computer Virus Catalog, published by VTC-Hamburg. Get the file ftp.informatik.uni-hamburg.de:/pub/virus/texts/catalog/atarivir.zip		

Name: Batman		
Aliases: Batman	**Type:**	
Disk Location:	**Features:**	
Damage:	**Size:**	**See Also:**
Notes: virus-l, v5-187 talks about it (see summary section)		

Name: Frankie		
Aliases: Frankie	**Type:**	
Disk Location: Applications and the Finder	**Features:**	
Damage:	**Size:**	**See Also:**
Notes:		

Name: Ghost		
Aliases: Ghost, Mouse Inversion	**Type:**	
Disk Location:	**Features:**	
Damage: Corrupts boot sector	**Size:**	**See Also:**
Notes: Does not check boot sectors to determine if they are already executable. It hooks itself into the ST operating system and writes a copy of itself onto every disk the ST reads or writes. It will overwrite any boot sector, rendering other booting disks useless. ST Virus Killer was able to clean up the affected disk and the virus apparently has not spread on the test system. It acts by counting how man copies of itself it has written. After 5 copies are made it starts attacking. Every 5 times the boot sector of either floppy is accessed, it reverses the vertical orientation of the mouse.		

In-Process Table

Viruses to be Described in Subsequent Update Bulletins

Aliases, 1381, 1605, 2131, 646, Vienna C, Arusiek, Barrotes, Bobo, calc, Christmas in Japan, Xmas in Japan, Cursy, Darkray, Dot Killer, 944, Point Killer, Dwi, Eddie 3, V651, Error Inc, Fairz, Fere Jacques, Fere, Halloechen, Holocaust, Honey, India, Inoc, Itavir, 3880, July 13th, June 16th, Pretoria, Korea, LBC Boot, Kukac,Turbo Kukac, Polish 2, Live After Death, V800, V800M, Lozinsky, Malmsey, Mark II, Marzia, Mayak, Microbes, Mr. D, Multichild, Music, Music Bug, Music Boot, Mystic, Necro-fear, Number 1, Number One, Phalcon.Emo, Ping Pong-C, Polimer, Polimat Tapeworm, Polish 217, 217, Polish Stupid, Polish 529, 529, Polish 529, Polish 583, Polish 961, Stone '90, Predator, Prudents Virus, 1210, Rape, Recovery Virus, 382, 382 Recovery Virus, Sarov, Scott's Valley, 2133, Screen+1, Seat, serene, shoo, Skater, Slow, Slowdown, Sorry, G-Virus V1.3, Soupy, Spyer, Student, Sverdlov, SVir, SVir-A, SVir-B, Svm, Ten Bytes, 1554, 1559, 9800:0000, V-Alert, Tequila, Turbo 448, @ Virus, Turbo @, Polish 2, UScan Virus, V2100, 2100, Velvet, VHP2, 623, VHP-623, VHP-627, Victor, Violator, Violator Strain B, VP, Yankee 2, 1624, 1961, Yankee go Home, Zherkov

MS-DOS/PC-DOS Cross Reference Table

This is the PC-DOS/MS-DOS virus name cross reference table. Use it to locate virus descriptions in the PC-DOS/MS-DOS virus description table. Locate the virus by name in the first column of this table then use the name in the second column to locate the virus description.

Virus Name/Alias	Name in Description
10 past 3	10 past 3
100 Years Virus	4096
1008	Oulu
1024	Diamond
1024-B	Nomenklatura
1024PrScr	1024PrScr
109 Virus	109 Virus
1160	Horse II
1168	Datacrime-B
1193	Copyright
12-TRICKS Trojan	12-TRICKS Trojan
1226	1226
1226D	1226
1226M	1226
1260	1260
1280	Datacrime
1391	Wordswap 1485
1392	Amoeba
1514	Datacrime II
1530	Chile Medeira
1536	Zero Bug
1539	Christmas
1575	Green Caterpillar
1590	Green Caterpillar
1591	Green Caterpillar
15xx	Green Caterpillar
1701	1701
1704	Cascade
1704 B	Cascade
1704 C	Cascade
1704-Format	1704-Format
1720	PSQR
17Y4	Cascade
1808	Jerusalem
1813	Jerusalem
1917	Datacrime II-B
1971	Eight Tunes
2080	Fu Manchu
2086	Fu Manchu
2387	2387
2576	Taiwan
2761	Advent
2930	Traceback II
2930-B	Traceback II
2KB	Jumper
2UP	2UP
3012	Plastique
3066	Traceback
3066-B	Traceback
3066-B2	Traceback
33	Thirty-three
333	Kennedy
3551	Macho
3555	Macho
382 Recovery	Recovery Virus
3APA3A	3APA3A
3X3SHR	3X3SHR
3y	3y
4-days	4-days
405	405
4096	4096
437	VFSI
45	minimal
453	RPVS
4711	Perfume
4870 Overwriting	4870 Overwriting
4res	4res
500 Virus	Merritt
505	Burger
509	Burger
512	Friday 13 th COM
512 Virus	Friday 13 th COM
512-A	512
512-B	512
512-C	512

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
512-D	512
5120	The Basic Virus
516	USSR
541	Burger
560-A	Burger
560-B	Burger
560-C	Burger
560-D	Burger
560-E	Burger
560-F	Burger
560-G	Burger
560-H	Burger
62-B	Vienna
632	Saratoga
637	Vcomm
640K Virus	Do Nothing
642	Icelandic II
648	Vienna
648-B	Vienna
66a	66a
688	Flash
765	Perfume
8-Tunes	Eight Tunes
800	Bulgarian 800
805	Stardot
847	Pixel
855	November 17
867	Typo
8920	Print Screen
909090H	Burger
910129	Brunswick
914	Russian Mutant
941	Devil's Dance
951	Devil's Dance
99%	99%
99 percent	99%
A-204	Jerusalem-B
A-Tel	Telefonica
A-VIR	Antitelifonica
Abacus	Vienna
Abbas	Abbas
Abraxas	Abraxas
Ada	DenZuk
Adolf	Adolf
Adolph\	V2P6
Advent	Advent
Advert	Pixel
Agiplan	Zero Bug
AIDS	AIDS
AIDS II	AIDS II
AIDS-II	AIDS II
Aircop	Aircop
Akuku	Akuku
Alabama	Alabama

Virus Name/Alias	Name in Description
Alabama.C	Alabama
Alabama-B	Alabama
Alameda	Merritt
Albania	Albania
Alex	Alex
Alexander	Alexander
Alfa	Diamond
Aliases	
Alien	PS-MPC
Ambulance Car	Ambulance Car
Ambulance.E	Ambulance Car
AmiLia	Murphy HIV
Amoeba	Maltese Amoeba
AMSES	Stealth B
Amstrad	Pixel
Anarchy.9594	Anarchy.9594
Anarkia	Jerusalem-B
Anarkia-B	Jerusalem-B
Andriyshka	Andryushka
Andro	Andro
Andromeda	Andromeda
Andryushka	Andryushka
Angarsk	Angarsk
Angelina	Angelina
Animus	Cookie
Anna	Anna
Anthrax	Anthrax
Anthrax PT	Anthrax
Anti CMOS	AntiCMOS
Anti EXE	AntiEXE
Anti Pascal	Anti Pascal
Anti Pascal 529	Anti Pascal
Anti Pascal 605	Anti Pascal
Anti-Gif	Virus Creation Lab
Anti-Pascal 400	AntiPascal II
Anti-Pascal 440	AntiPascal II
Anti-Pascal 480	AntiPascal II
Anti-pascal II	AntiPascal II
ANTI-PCB	ANTI-PCB
Anti-Tel	Telefonica
AntiCAD	AntiCAD
AntiCMOS	AntiCMOS
AntiCMOS.B	AntiCMOS
AntiEXE	AntiEXE
AntiEXE.A	AntiEXE
Antiline	HLLC
Antimon	Antimon
AntiPascal	AntiPascal
AntiPascal II	AntiPascal II
Antitelifonica	Antitelifonica
Antix Trojan	Antix Trojan
aol gold	AOLGOLD

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
AOLGOLD	AOLGOLD
aolgold.zip	AOLGOLD
AP 529	Anti Pascal
AP 605	Anti Pascal
AP-400	AntiPascal II
AP-440	AntiPascal II
AP-480	AntiPascal II
Apilapil	EUPM
Apocalypse-2	Dark Avenger
April 1. EXE	April 1. EXE
April 15	Murphy-1
April 1st	Suriv-01
April-1-COM	Suriv-01
Arab	Jerusalem-B
Arab Star	Jerusalem-B
Aragon	Aragon
ARC513.EXE	ARC513.EXE
ARC514.COM	ARC513.EXE
ARC533	ARC533
Arcv.companion	Arcv.companion
Arcv-9	PS-MPC
Armagedon	Armagedon
Armagedon the first	Armagedon
Armagedon the Greek	Armagedon
Arriba	Arriba
Ash	Ash
Ash-743	Ash
Ashar	Brain
Ashar_B	Brain
Astra	Astra
AT	AT
AT II	AT II
Atas	Atas
Athens	Athens
Atomic	Atomic
Attention	Attention
Attention!	Attention
Attention.C	Attention
Aurea	Aurea
Australian	Jerusalem
Australian Parasite.272	Australian Parasite.272
Austrian	Vienna
Auto	Auto
Autumn	Cascade
AZUSA	AZUSA
Azuza	AZUSA
B1	New York Boot
Backfont	Backfont
BACKTALK	BACKTALK
Bad Boy	Bad Boy
Bad Sector	BadSector
BADDISK	DISKSCAN

Virus Name/Alias	Name in Description
BadSector	BadSector
Baobab	Baobab
Barrotes	Barrotes
Beast C	Number of the Beast
Beast D	Number of the Beast
Bebe	Bebe
Bebe-486	Bebe
Beijing	Bloody!
Best Wish (may be wrong)	Troi
Best Wishes	Best Wishes
Best Wishes-970	Best Wishes
Best Wishes-B	Best Wishes
Beta	Bob Ross
BetaBoys	BetaBoys
Better World	Fellowship
Beware	Beware
BFD	BFD
Big Caibua	BUTTHEAD
Big Joke	Big Joke
BIO	BIO
Bit Addict	Bit Addict
Black Avenger	Dark Avenger
Black Friday	Jerusalem
Black Hole	Jerusalem
Black Jec	Black Jec
Black Knight	Prot-T.Lockjaw.2
Black Monday	Black Monday
Blackbox	Jerusalem
Blackjack	Cascade
Blood	Blood
Blood 2	Blood
Blood Rage	Blood Rage
BloodLust	BloodLust
BloodRage	Blood Rage
Bloody!	Bloody!
Bloomington	Bloomington
Blue_Nine	Blue_Nine
Blue Nine	Blue_Nine
Bob	Bob Ross
Bob Ross	Bob Ross
Bones	Bones
Boojum	Boojum
Boot	Ping Pong B
Boot 437	Boot 437
boot-437	Boot 437
Boot-EXE	BFD
Borderline	Black Monday
Bouncing Ball	Ping Pong
Bouncing Dot	Ping Pong
Boys	Boys
Brain	Brain
@BRAIN	Brain
Brainy	Warrier

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Brasil Virus	Brasil Virus
Brazil	Brasil Virus
Breeder	Breeder
Brenda	Kennedy
Brunswick	Brunswick
Bryansk	Bryansk
BUA-2263	BUTTHEAD
Bubbles	IVP
Budo	Budo
Bulgarian	Plovdiv
Bulgarian 800	Bulgarian 800
Bulgarian Damage 1.3	Plovdiv
BUPT	BUPT
Buptboot	Buptboot
Burger	Burger
Burger 382	Burger
Burger 405	Burger
Burghoffer	Burghoffer
Bush	Vienna
Bustard	Burger
Butterfly	Butterfly
BUTTHEAD	BUTTHEAD
ByeBye	Virus Creation Lab
C 605	Anti Pascal
C virus	Cascade
C-544	C-544
Caco	Caco
Camouflage	1260
Campana	Telefonica
Campanja	Telefonica
Cancer	Smiley Cancer
Cansu	Cansu
Capital	Capital
CARA	CARA
Carbuncle	Carbuncle
Carioca	Carioca
CARMEL TntVirus	CARMEL TntVirus
Cascade	Cascade
Cascade A	Cascade
Cascade B	Cascade
Cascade Format	1704-Format
Cascade YAP	Cascade
Casino	Casino
Casper	Casper
Catch 22	Catch 22
Catch-22	Catch 22
CAZ	CAZ
CAZ-1159	CAZ
CB-1530	Dark Avenger
CC	CC
CD-IT.ZIP	Warpcom-II
CDIR	CDIR
Century	4096

Virus Name/Alias	Name in Description
Century Virus	4096
Chad	Chad
Chameleon	1260
Chaos	Chaos
Cheater	Burger
Checksum	Checksum
Checksum 1.01	Checksum
Cheeba	Cheeba
Chemnitz	Chemnitz
Chile Medeira	Chile Medeira
Chinese Fish	Chinese Fish
Chinese_Fish	Chinese Fish
Chinon	Warpcom-II
Choinka	Vienna
Chris	Chris
Christmas	Christmas
Christmas Tree	Christmas
CIA	Burger
Cinderella	Cinderella
Cinderella II	Cinderella
Civil War	Civilwar
Civil War III	Civilwar
Civilwar	Civilwar
Clinton	Leprosy
Clone	Mirror
Clonewar	Clonewar
Close	Close
Cls	Cls
Cluster	Dir II
CMOS4.	AntiEXE
Cod	Cod
Code Zero	Code Zero
CoffeeShop	Mutation Engine
Coib	Coib
College	College
Columbus Day	Datacrime
COM Virus	Friday 13 th COM
Com2con	Com2con
Comasp-472	Comasp-472
Commander Bomber	Commander Bomber
Como	Como
Compiler.1	Compiler.1
Computer Ogre	Disk Killer
Cookie	Cookie
Copmpl	Akuku
Copyright	Copyright
Cossiga	Cossiga
CPL35.COM	CPL35.COM
CPW	Cpw
Cpw	Cpw
Crackpot-1951	Murphy-1
Crackpot-272	Murphy-1
Cracky	Cracky
Crazy	Crazy Eddie

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Crazy Eddie	Crazy Eddie
Crazy Imp	Crazy Imp
Crazy_Nine	Crazy_Nine
Creeper	Creeper
Creeper-425	Creeper
Creeping Death	Dir II
Creeping Tormentor	Creeper
Crew-2048	Crew-2048
Crime	Datacrime
Crime-2B	Datacrime II-B
Criminal	Ultimate Weapon
Crooked	Crooked
Cruncher	Cruncher
Cruncher 1.0	Cruncher
Cruncher 2.0	Cruncher
Cruncher 2.1	Cruncher
Crusades	Butterfly
Crusher	Crusher
CryptLab	Mutation Engine
Cryptlab	Mutation Engine
CSL	CSL
CSL-V4	CSL
CSL-V5	CSL
Cunning	Cascade
Cursy	Cursy
Cybercide	Cybercide
CyberTech	CyberTech
D-XREF60.COM	D-XREF60.COM
D2	Dir II
D3	AntiEXE
da	Dada
Da Boys	Da'Boys
Da'Boys	Da'Boys
DaBoys	Da'Boys
Dada	Dada
Dallas Cowboys	Da'Boys
Damage	Plovdiv
Damage 1.1	Plovdiv
Damage 1.3	Plovdiv
Damage-2	Diamond
DAME	Mutation Engine
DAME (Dark Avenger Mutation Engine)	Mutation Engine
DANCERS	DANCERS
DANCERS.BAS	DANCERS
Danish Tiny	Kennedy
Dark Apocalypse	Dark Apocalypse
Dark Avenger	Dark Avenger
Dark_Avenger.1800.A	Dark Avenger
Dark Avenger 3	Dark Avenger 3
Dark Avenger II	Dark Avenger 3
Dark Avenger III	Dark Avenger 3
Dark Avenger's Latest	Mutation Engine
Dark Avenger-B	Dark Avenger
Dark End	Dark End
Dark Helmet	Civilwar
Dark Lord	Terror
Darth Vader	Darth Vader
Dash-em	Dash-em
Dashel	Dashel
Datacrime	Datacrime
Datacrime Ia	Datacrime-B
DATACRIME Ib	Datacrime
Datacrime II	Datacrime II
Datacrime II-B	Datacrime II-B
Datacrime-B	Datacrime-B
Datalock	Datalock
Datalock 1.00	Datalock
Datalock 2	Datalock
Datalock-1043	Datalock
David	Diamond
Day10	Day10
Dbase	Dbase
DBF virus	Dbase
Dead Kennedy	Kennedy
Death to Pascal	Wisconsin
December 24th	Icelandic III
Decide	Deicide
Dedicated	Mutation Engine
Deicide	Deicide
Deicide II	Deicide
Dejmi	Dejmi
Demolition	Demolition
Demon	Murphy-1
Den Zuk	DenZuk
Den Zuk 2	Ohio
Den-Zuk 2	Ohio
DenZuc B	DenZuk
DenZuk	DenZuk
Denzuko	DenZuk
Deranged	PS-MPC
derived of Stoned	Empire B.2
Destructor	Destructor
Devil's Dance	Devil's Dance
Dewdz	Dewdz
DH2	Die Hard
Diamond	Diamond
Diana	Dark Avenger
Dichotomy	Dichotomy
Die Hard	Die Hard
Die_Hard. Diehard	Die Hard
Die Young	Dark Avenger 3
Digger	Digger
Digital F/X	Black Jec
Dima	Dima

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
DIR	Dir II
Dir 2	Dir II
Dir II	Dir II
Dir2	Dir II
Disk Crunching Virus	Icelandic
Disk Eating Virus	Icelandic
Disk Killer	Disk Killer
Disk Ogre	Disk Killer
DISKSCAN	DISKSCAN
Diskspoiler	Diskspoiler
Dismember	Dismember
DM	DM
DM-310	DM
DM-330	DM
DMASTER	DMASTER
Do Nothing	Do Nothing
Doom	Doom
Doom II	Doom
Doom-2B	Doom
Doomsday	Doomsday
Dos 7	Dos 7
DOS-62	Vienna
Dos-62	Vienna
DOS-68	Vienna
DOS-HELP	DOS-HELP
Dos3	PS-MPC
DOShunt	DOShunt
DOSKNOWS	DOSKNOWS
Dosver	Dosver
Dot Killer	Dot Killer
Doteater	Doteater
DPROTECT	DPROTECT
Dracula	Dracula
Dragon	Totoro Dragon
DRAIN2	DRAIN2
DRIVER-1024	Dir II
DROID	DROID
Dropper 7	Dropper7
Dropper7	Dropper7
Dropper7 boot	Dropper7 boot
DRPTR	DRPTR
DSZBREAK	DSZBREAK
Du	Du
Ducklin	Stinkfoot
Dudley	Dudley
Durban	Durban
Dutch 424	Europe '92
Dutch Tiny	Dutch Tiny
Dutch Tiny-124	Dutch Tiny
Dutch Tiny-99	Dutch Tiny
Dy	Dy
Dyslexia	Solano 2000
Dyslexia 2.00	Solano 2000
Dyslexia 2.01	Solano 2000
Dzino	Dzino
E. T. C.	E. T. C.
E-Rillutanza	E-Rillutanza
Ear	Ear
Earthquake	Virus Creation Lab
Eastern Digital	Eastern Digital
EB-21	Print Screen
Ecu	PS-MPC
Eddie	Dark Avenger
Eddie 2	Eddie 2
Eddie 3	Dark Avenger 3
EDV	EDV
EE	Jumper
EGABTR	EGABTR
Eight Tunes	Eight Tunes
Eliza	Eliza
EM	EM
EMF	EMF
Emma	Emma
Emmie	Emmie
Empire	Empire
Empire A	Empire
Empire B.2	Empire
Empire C	Empire
Empire D	Empire
Encroacher	Encroacher
End of	End of
ENET 37	Friday 13 th COM
Enigma	Yankee Doodle
Enola	Enola
Essex	QRry
EUPM	EUPM
Europe '92	Europe '92
European Fish	Fish
Even Beeper	HLLC
Evil	V1701New
Evil Avatar	Dichotomy
Evil-B	V1701New
exe_bug	EXEBUG
EXEBUG	EXEBUG
EXEBUG1	EXEBUG
EXEBUG2	EXEBUG
EXEBUG3	EXEBUG
Explosion-II	One_half
Exterminator	Murphy-1
F-Soft	F-Soft
F-Soft 563	F-Soft
F-Word	F-Word
F-you	F-Word
F1-337	F1-337
Faerie	Faerie
Faggot	VHP

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Fall	Cascade
Falling Leaves	Cascade
Falling Letters	Ping Pong B
Falling Letters Boot	Ping Pong B
Falling Tears	Cascade
FAT EATER	MAP
Father Christmas	Christmas
Faust	Chaos
Fax Free	Fax Free
FCB	FCB
Fear	Mutation Engine
Feist	Feist
Fellowship	Fellowship
FGT	FGT
Fichv	Fichv
Fichv-EXE 1.0	Fichv
Filedate 11	Filedate 11
Filedate 11-537	Filedate 11
FILES.GBS	FILES.GBS
Filler	Filler
Finnish	Finnish
Finnish-357	Finnish
Fish	Fish
Fish 6	Fish
Fist.927	Sticky
Five O'Clock	Yankee Doodle
FIXIT	MATHKIDS
Flash	Flash
Flex	PS-MPC
Flip	Flip
Flip Clone	Mirror
Flower	Flower
FLU4TXT	FLUSHOT4
FLUSHOT4	FLUSHOT4
Forger	Forger
Form	Form
Form Boot	Form
FORM-Virus	Form
Formiche	Cascade
Forms	Form
France	Paris
Freddy	Freddy
Free Agent	Free Agent
Freelove	One_half
Freew	Freew
French Boot	Jumper
Friday 13 th COM	Friday 13 th COM
Friday 13th	Jerusalem
Friday The 13th-B	Friday 13 th COM
Friday The 13th-C	Friday 13 th COM
Friends	Cossiga
Frodo	4096
Frodo Soft	F-Soft
Frog's Alley	Frog's Alley

Virus Name/Alias	Name in Description
Frogs	Frogs
Fruit-Fly	Satan Bug
Fu Manchu	Fu Manchu
Fuck You	F-Word
Fumanchu	Fu Manchu
Fumble	Typo
Funeral	Funeral
FUTURE	FUTURE
G-MAN	G-MAN
GATEWAY	GATEWAY
GATEWAY2	GATEWAY
Geek	Geek
Gemand	Gemand
Gen B	LZR
Genb	Genb
GenBP	LZR
Genc	Genc
Generic Boot	Genb
GenericBoot	Genb
genp	Genb
Gergana	Gergana
Gergana-222	Gergana
Gergana-300	Gergana
Gergana-450	Gergana
Gergana-512	Gergana
Geschenk	PS-MPC
Ghost	Ghost
Ghost Boot	GhostBalls
Ghost COM	GhostBalls
GhostBalls	GhostBalls
Girafe	Girafe
Gliss	Gliss
Globe	Globe
GMB	HH&H
Goblin	Murphy-1
Goddam Butterflies	Butterfly
Goga	Goga
Gold_Bug	Gold_Bug
Gold Bug	Gold_Bug
Goldbug	Goldbug
Golden Gate	Merritt
Golgi	Golgi
Gomb	HH&H
Good Times	Good Times
Good_Times	Good Times
GoodTimes	Good Times
Gosia	Gosia
Got You	Got You
GOT319.COM	GOT319.COM
Gotcha	Gotcha
Gotcha-D	Gotcha
Gotcha-E	Gotcha
GRABBER	GRABBER
Grain of Sand	Maltese Amoeba

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Granada	Granada
Grease	PS-MPC
Greemlin	Diamond
Green Caterpillar	Green Caterpillar
Green Left	Groen
Groen	Groen
Groen Links	Groen
Grog	Grog
Groove	Mutation Engine
Grower	Grower
Grune	Grune
Gulf War	Gulf War
Guppy	Guppy
Gyorgy	Flash
Gyro	Gyro
Ha!	Ha!
Ha	Ha!
Hacker	DenZuk
Haddock	Haddock
Hafenstrasse	Hafenstrasse
Hahaha	AIDS
Haifa	Haifa
Halloechen	Halloechen
Halloechn	Halloechen
Happy	Joshi
Happy Birthday Joshi	Joshi
Happy Days Trojan	Happy Days Trojan
Happy Halloween	Happy Halloween
Happy Monday	Happy Monday
Happy New Year	Happy New Year
Harakiri	Harakiri
Hary Anto	Hary Anto
Hate	Hate
Hates	Hates
Havoc	Neuroquila
Hawaii	Stoned
HD Trojan	Happy Days Trojan
Headcrash	Headcrash
Hebrew University	Jerusalem
Hello	Halloechen
Hello_1a	Halloechen
Helloween	Helloween
Hemp	Stoned
Herbst	Cascade
Hero	Hero
Hero-394	Hero
Hey You	Hey You
HH&H	HH&H
Hi	Hi
Hide and Seek	Hide and Seek
Hidenowt	Hidenowt
Highlander	Highlander
Hitchcock	Hitchcock

Virus Name/Alias	Name in Description
HLLC	HLLC
HM2	Plastique
Holland Girl	Sylvia V2.1
Holo	Kamp
Hong Kong	AZUSA
Horror	Horror
Horse	Horse II
Horse Boot virus	Horse Boot virus
Horse II	Horse II
Houston B1	Houston B1
Hungarian	Hungarian
Hungarian-473	Hungarian
Hydra	Hydra
Hymn	Hymn
Icelandic	Icelandic
Icelandic II	Icelandic II
Icelandic III	Icelandic III
IDF	4096
Imp	Crazy Imp
Infector	November 17
Int_10	Int_10
Intruder	Intruder
Invader	Invader
Invol	Invol
Involuntary	Involuntary
INVOLVE	INVOLVE
Irish	Maltese Amoeba
Iron Hoof	PS-MPC
Israeli	Jerusalem
Israeli #3	Suriv-03
Israeli Boot	Israeli Boot
Italian	Ping Pong
Italian Boy	Italian Boy
Italian Diamond	Diamond
IVP	IVP
IWG	Vienna
Jack Ripper	Jack the Ripper
Jack the Ripper	Jack the Ripper
Jackal	Jackal
Japanese_Christmas	Japanese_Christmas
Jeff	Jeff
Jericho	Dark Avenger
Jerusalem	Jerusalem
Jerusalem A	Jerusalem
Jerusalem (B)	Suriv-03
Jerusalem variant	Jerusalem
Jerusalem-B	Jerusalem-B
Jerusalem-C	Jerusalem-B
Jerusalem-D	Jerusalem-B
Jerusalem-DC	Jerusalem-B
Jerusalem-E	Jerusalem-B
Jerusalem-E2	Jerusalem-B
Jest	Jest
Jo	PS-MPC

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Jo-Jo	Cascade
Jocker	Joker
Joe's Demise	Joe's Demise
Joes Demise	Joe's Demise
Joker	Joker
Joker 2	JOKER-01
JOKER-01	JOKER-01
Joker-01 Joker 01	JOKER-01
Jork	Brain
Joshi	Joshi
Jumper	Jumper
Jumper B	Jumper
June 4th	Bloody!
JUNKIE	JUNKIE
Justice	Justice
K-4	K-4
Kamikazi	Kamikazi
Kamp	Kamp
Kamp-3700	Kamp
Kamp-3784	Kamp
Kampana	Telefonica
Kaos 4	KAOS4
KAOS4	KAOS4
Kemerovo	Kemerovo
Kennedy	Kennedy
Kernel	Kernel
KEYBGR Trojan	Scrambler
Keypress	Keypress
King of Hearts	KOH
Klaeren	Hate
Knight	Prot-T.Lockjaw.2
KOH	KOH
Krivmous	Crooked
Kylie (variant)	Jerusalem
Lapse	Lapse
Leapfrog	Leapfrog
Lehigh	Lehigh
Lehigh-2	Lehigh
Lehigh-B	Lehigh
Lenart	AntiCMOS
Leningrad	Leningrad
Leprosy	Leprosy
Leprosy 1.00	Leprosy
Leprosy-B	Leprosy
Liberty	Liberty
Liberty-B	Liberty
Liberty-C	Liberty
Lima	Burger
Lisbon	Vienna
Literak	Literak
Little Girl	Little Girl
Little Red	Little Red
Little.Red	Little Red
Lock-up	Lock-up

Virus Name/Alias	Name in Description
Lockjaw-zwei	Prot-T.Lockjaw.2
Loki	Loki
LOKJAW-ZWEI	Prot-T.Lockjaw.2
Lor	Grog
Loren	Loren
Lucifer	Diamond
Lyceum	Lyceum
LZ	LZ
LZR	LZR
M_jmp	M_jmp
MacGyver	MacGyver
Macho	Macho
MachoSoft	Macho
Macrosoft	Syslock
Mad Satan	MacGyver
Magician	Magician
Malta	Casino
Maltese Amoeba	Maltese Amoeba
Mandela	IVP
Manuel	Manuel
Mao	Little Red
MAP	MAP
Marauder	Marauder
Mardi Bros	DenZuk
Marijuana	Stoned
Markt	Markt
Math	IVP
MATHKIDS	MATHKIDS
Matura	Matura
Mazatlan	Merritt
Mcgy	MacGyver
McGyver	MacGyver
McWhale	PS-MPC
Mediera	Chile Medeira
Mel	Mel
Mendoza	Jerusalem-B
Merritt	Merritt
Merry Christmas	Merry Christmas
Metal Thunder	Akuku
Mexican	Devil's Dance
Mexican Stoned	Mexican Stoned
MG series II	Dir II
MGTU	MGTU
Miami	Friday 13 th COM
Mich	Michelangelo
Michaelangelo	Michelangelo
Michelangelo	Michelangelo
Microelephant	CSL
Mierda?	Chile Medeira
Milan	Milan
Milan.WWT.67.C	Milan
Milana	Dark Avenger
Milena	Milena
minimal	minimal

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
minimal-45	minimal
Minimite	Minimite
Minnow	ZeroHunt
MIR	Dark Avenger
Mirror	Mirror
Mistake	Typo
MIX/1	Mix1
Mix1	Mix1
MIX1	Mix1
Mixer1	Mix1
Moctzuma	Moctzuma
Moctzuma-B	Moctzuma
Modem virus of 1989	Modem virus of 1989
Mon	Monkey
Monday 1st	Beware
Monkey	Monkey
Monxla A	Monxla A
Monxla B	Monxla A
Moose	Moose
Moose31	Moose
Moose32	Moose
Mosquito	Fax Free
Mother Fish	Whale
MPS-OPC II	MPS-OPC II
Mr. G	Mr. G
Mshark	Mshark
MtE	Mutation Engine
Mud	BetaBoys
Mule	Jerusalem
Multi	Multi
Multi2	Sticky
Mummy	Mummy
Munich	Friday 13 th COM
Murphy	Murphy-1
Murphy HIV	Murphy HIV
Murphy variant	Murphy HIV
Murphy-1	Murphy-1
Murphy-2	Murphy-2
Music	Oropax
Musician	Oropax
Mutation Engine	Mutation Engine
Mutator	Mutator
N8FALL	N8FALL
Napolean	PS-MPC
Natas	Natas
Naught	Naught
Naughty Hacker	Horse
Near_End	Pixel
Net Crasher	Net Crasher
Neuro.Havoc	Neuroquila
Neuroquila	Neuroquila
Neuville	Jumper
Never Mind	Never Mind
New Bug	Genb
New Jerusalem	Jerusalem-B
New York Boot	New York Boot
New Zealand	Stoned
NewBug	Genb
News Flash	Leprosy
Nice Day	Nice Day
Nina	Nina
Nina-2	Happy New Year
Nirvana	PS-MPC
NMAN	NMAN
NMAN B	NMAN
NMAN C	NMAN
No Bock	No Bock
No Frills	No Frills
No_Smoking	No_Smoking
NOINT	Bloomington
Nomenklatura	Nomenklatura
NOP	Bones
Nostardamus	Nostardamus
(not really) Simplistic File Infector	November 17
NOTROJ	NOTROJ
Nov 17	November 17
Nov. 17	November 17
Nov 17-768	November 17
Nov 17-800	November 17
Nov 17-880	November 17
Nov 17-B	November 17
Novell	Novell
November 17	November 17
November 30	November 30
Nowhere Man	NMAN
NPox	NukePox
Npox.1482	Npox.1482
Nu_Way	Sticky
Nuke5	PS-MPC
NukePox	NukePox
Null Set	Doomsday
Number of the Beast	Number of the Beast
NYB	New York Boot
Nygus	Nygus
Nympho	Nympho
odud	Dudley
Off-Road	Off-Road
Ohio	DenZuk
Oi Dudley	Dudley
OK	OK
Old Yankee	Yankee Doodle
Omega	Omega
Omicron	Flip
Omicron PT	Flip
One_half	One_half
one half	One_half
One In Ten	Icelandic

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
One In Two	Saratoga
Only	Crooked
Ontario	Ontario
Oropax	Oropax
Osiris	Osiris
Oulu	Oulu
Outland	Dark Avenger
Override	Override
P1	Phoenix
PACKDIR	PACKDIR
Page	PS-MPC
Pakistani	Brain
Palette	Zero Bug
Pandaflu	Antimon
Paniker	C-544
Paranoramia	Virus Creation Lab
Paris	Paris
Parity	Parity 2
Parity 2	Parity 2
Parity Boot	Parity 2
Parity_Boot.A and Parity_Boot.B	Parity 2
Park ESS	Jerusalem-B
Particle Man	Particle Man
Pathogen	Smeg
Patricia	Murphy-1
Paul Ducklin	Stinkfoot
Payday	Jerusalem-B
PC Flu 2	PC Flu 2
PC Weevil	PC Weevil
PC-WRITE 2.71	PCW271
PCW271	PCW271
Peach	Peach
Peanut	Peanut
Peking	Merritt
Pentagon	Pentagon
Perfume	Perfume
Perry	Perry
Phoenix	1226
Phoenix D	Phoenix D
(Phoenix related)	1226
Phoenix related	1226
Phx	Phx
Ping Pong	Ping Pong
Ping Pong B	Ping Pong B
Pirate	Burger
Pisello	Fax Free
Pit	Pit
Pixel	Pixel
PK362	PKPAK/PKUNPAK 3.61
PK363	PKPAK/PKUNPAK 3.61
PKB35B35	PKX35B35
PKFIX361	PKFIX361
PKPAK/PKUNPAK 3.61	PKPAK/PKUNPAK 3.61
PKX35B35	PKX35B35
PKZ201.EXE	PKZIP Trojan 1
PKZ201.ZIP	PKZIP Trojan 1
PKZIP Trojan 1	PKZIP Trojan 1
PKZIP Trojan 2	PKZIP Trojan 2
PKZIPV2.EXE	PKZIP Trojan 2
PKZIPV2.ZIP	PKZIP Trojan 2
Plague	Plague
Plastic Boot	Invader
Plastique	Plastique
Plastique 1	Plastique
Plastique 2	AntiCAD
Plastique 4.51	Plastique
Plastique 5.21	AntiCAD
Plastique-B	AntiCAD
PLO	Jerusalem
Plovdiv	Plovdiv
Plovdiv 1.1	Plovdiv
Plovdiv 1.3	Plovdiv
Pogue	Mutation Engine
Point Killer	Dot Killer
Poisoning	Virus Creation Lab
Pojer	Pixel
Possessed	Possessed
Possessed A	Possessed
Possessed B	Possessed
Potassium Hydroxide	KOH
Print Screen	Print Screen
Print Screen 2	Print Screen
Prot-T.Lockjaw.2	Prot-T.Lockjaw.2
Proto-T.Flagyll.371	Proto-T.Flagyll.371
proton	proton
Proud	Proud
PrSc	1024PrScr
PrScr	1024PrScr
PrtSc	Print Screen
Ps!ko	Dark Avenger
PS-MPC	PS-MPC
PSQR	PSQR
Puerto	Jerusalem-B
QRry	QRry
Quadratic	Quadratic
Quake	Ear
Queeg	Smeg
Questo	Mutation Engine
Quicksilver.1376	Quicky
Quicky	Quicky
QUIKRBBS	QUIKRBBS
QUIKREF	QUIKREF
Quox	Quox
Rabid	Dark Avenger

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Radyum	Radyum
RAM	RAM
Rape	Rape
Rapid Avenger	Dark Avenger
Rasek	Rasek
RCKVIDEO	RCKVIDEO
Red Cross	Ambulance Car
Red Diavolyata	Red Diavolyata
REDX	Ambulance Car
Relzfu	Relzfu
Retribution	Retribution
Rillutanza	E-Rillutanza
Ripper	Jack the Ripper
RMNS	RMNS
RMNS MW	RMNS
Rock Steady	Diamond
RPVS	RPVS
RPVS-B	RPVS
Russian	Jerusalem
Russian_Mirror	Russian_Mirror
Russian Mutant	Russian Mutant
S-Bug	Satan Bug
Sad	Black Jec
Saddam	Saddam
Sampo	Sampo
San Diego	Stoned
Sara	Mutation Engine
Sarah	Mutation Engine
Saratoga	Icelandic
Saratoga 2	Icelandic
Sat_Bug	Satan Bug
Sata	Sata
Satan	Satan Bug
Satan Bug	Satan Bug
SatanBug	Satan Bug
Saturday the 14th	Durban
Satyricon	Satyricon
SBC	SBC
SBC-1024	SBC
SCANBAD	DISKSCAN
Scion	Doomsday
Scott's Valley	Jerusalem
Scrambler	Scrambler
Screaming Fist	Screaming Fist
Scroll	PS-MPC
Search	DenZuk
SECRET	SECRET
SECURE.COM	SECURE.COM
(see also Antitelefonica)	Telefonica
Sentinel	Sentinel
Seoul	Merritt
Sexotica	KAOS4
SF Virus	Merritt

Virus Name/Alias	Name in Description
Shake	Shake
Shanghai	Shanghai
Shield	Breeder
Shifter	Shifter
Shiny	PS-MPC
Shoe	Brain
Shoe B	Brain
Shoe_Virus	Brain
Shoe_Virus_B	Brain
Shoo	shoo
SI-492	SI-492
SIDEWAYS	SIDEWAYS
SIDEWAYS.COM	SIDEWAYS
Sigalit	Cansu
Sillybob	Jumper
SillyC	SillyC
SillyOR	SillyOR
Silo	IVP
Simulation	Simulation
Sistor	Sistor
Skeleton	PS-MPC
Skew	Skew
Skism-1	Jerusalem-B
Slime	PS-MPC
Slovak Bomber	One_half
Slovakia	Slovakia
Slow	Jerusalem
Slub	Slub
Smack	Murphy-1
Smeg	Smeg
Smithsonian	Stoned
Smoka	Smoka
Smulders's virus	Ultimate Weapon
Sofia-Term	Sofia-Term
Solano 2000	Solano 2000
Soolution	PS-MPC
Sorlec4	PS-MPC
Sorlec5	PS-MPC
Soup	PS-MPC
South African	Friday 13 th COM
Spanish Telecom	Telefonica
Spectre	Spectre
Split	Split
Spring	Spring
Stamford	Stamford
STAR	Jerusalem-B
Stardot	Stardot
Starship	Starship
STB	Stealth B
Stealth	4096
Stealth 2 Boot	Quox
Stealth B	Stealth B
Stealth.B	Stealth B
StealthBoot-D	KOH

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Stelboo	Stealth B
Sterculius	Sterculius
Sticky	Sticky
Stigmata	Kennedy
Stimp	Stimp
Stinkfoot	Stinkfoot
Stoned	Stoned
stoned.1	New York Boot
Stoned 3	Bloomington
Stoned III	Bloomington
Stoned.LZR	LZR
Stoned variant	Stoned
stoned variant	Stoned
Stoned-B	Stoned
Stoned-C	Stoned
Stoned-T	Bones
Storm	Storm
STRIPES	STAR
stupid	Do Nothing
Stupid Jack	Murphy-1
Stupid.Sadam.Queit	Stupid.Sadam.Queit
Stupid Virus	Do Nothing
Subliminal	Solano 2000
Sudah ada vaksin	DenZuk
SUG	SUG
Suicide	Ear
Sunday	Sunday
Sunday-B	Sunday
Sunday-C	Sunday
Sundevil	Sundevil
Suomi	Oulu
sURIV 1.01	Suriv-01
Suriv 2	April 1. EXE
Suriv 2.01	April 1. EXE
Suriv 3.00	Suriv-03
Suriv A	Suriv-01
Suriv B	Suriv-03
Suriv-01	Suriv-01
Suriv-03	Suriv-03
Suriv03	Suriv-03
Surviv	Xuxa
SVC 6.0	SVC 6.0
Swami	Murphy-1
Swank	IVP
Swap	Israeli Boot
Swap Boot	Israeli Boot
Sybille	Sybille
Sylvia	Sylvia V2.1
Sylvia V2.1	Sylvia V2.1
SYP	Day10
Syslexia	Solano 2000
Syslock	Syslock
System Virus	Icelandic II
T-rex	PS-MPC

Virus Name/Alias	Name in Description
Tack	Tack
Tai-Pan	Tai-Pan
Taiwan	Taiwan
Taiwan 2	Taiwan
Taiwan 3	Taiwan
Taiwan 4	Taiwan
Taiwan-B	Taiwan
Tannenbaum	Christmas
Taunt	AIDS
Telecom 1	Kamp
Telecom 2	Kamp
Telecom Boot	Telefonica
Telefonica	Telefonica
Terror	Terror
Testvirus-B	Testvirus-B
The 648 Virus	Vienna
The Basic Virus	The Basic Virus
The One-in-Eight Virus	Vienna
The Second Austrian Virus	Cascade
Thirty-three	Thirty-three
Tic	Tic
Time Virus	Monxla A
timer	Free Agent
Timid	Timid
Timor	Jerusalem
Tiny 133	Tiny virus
Tiny 134	Tiny virus
Tiny 138	Tiny virus
Tiny 143	Tiny virus
Tiny 154	Tiny virus
Tiny 156	Tiny virus
Tiny 158	Tiny virus
Tiny 159	Tiny virus
Tiny 160	Tiny virus
Tiny 163	Tiny 163
Tiny 169	Tiny virus
Tiny 198	Tiny virus
Tiny virus	Tiny virus
TIRED	TIRED
Toast	PS-MPC
Tomato	Tomato
Toothless	Toothless
TOPDOS	TOPDOS
Topo	Fax Free
Totoro Cat	Totoro Dragon
Totoro Dragon	Totoro Dragon
Touche	Jumper
Toxic	Atomic
Toys	PS-MPC
TP04VIR	Vacsina
TP05VIR	Vacsina
TP06VIR	Vacsina

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
TP16VIR	Vacsina
TP23VIR	Vacsina
TP24VIR	Vacsina
TP25VIR	Vacsina
TP33VIR	Yankee Doodle
TP34VIR	Yankee Doodle
TP38VIR	Yankee Doodle
TP41VIR	Yankee Doodle
TP42VIR	Yankee Doodle
TP44VIR	Yankee Doodle
TP45VIR	Yankee Doodle
TP46VIR	Yankee Doodle
TPE	Girafe
TPWORM	TPWORM
Traceback	Traceback II
Traceback II	Traceback II
Traceback II-B	Traceback II
Traceback-B	Traceback
Traceback-B2	Traceback
Trackswap	Trackswap
Travel	Dark Avenger 3
Traveler	BUPT
Traveler Jack	Traveler Jack
Tremor	Tremor
Tremor2	Tremor
Tricks	12-TRICKS Trojan
Trident	Girafe
TridenT	Girafe
Trident Polymorphic Engine	TPE
Trigger	Trigger
Trivial	Trivial
Trivial-64	Trivial-64
Troi	Troi
Troi Two	Troi
TSRMAP	TSRMAP
TUQ	RPVS
Turbo	Turbo 448
Turin Virus	Ping Pong
Twelve Tricks Trojan	12-TRICKS Trojan
Twin-351	Twin-351
Type Boot	Typo
Typo	Typo
Typo COM	Typo
UIUC	Brain
UIUC-B	Brain
ULTIMATE	ULTIMATE
Ultimate Weapon	Ultimate Weapon
Ultimatum	Ultimatum
Unesco	Vienna
Unexe	Unexe
UofA	Empire
Uriel	Dark Avenger
Uruguay	Uruguay

Virus Name/Alias	Name in Description
Uruk Hai	Uruk Hai
USSR	USSR
USSR 1049	USSR
USSR 1594	USSR
USSR 1689	USSR
USSR 2144	USSR
USSR 516	USSR
USSR 600	USSR
USSR 707	USSR
USSR 711	USSR
USSR 948	USSR
USSR-311	Com2con
V	The Basic Virus
V.1376	Quicky
V 163	Tiny 163
V Basic Virus	The Basic Virus
V-163	Tiny 163
V-277	Viki
V-299	V-299
V-345	V-345
V-605	Anti Pascal
V-801	Stardot
V-847	Pixel
V-847B	Pixel
V-852	Pixel
V-sign	Cansu
V08-15	V08-15
v1024	Dark Avenger 3
V1226	1226
V1226D	1226
V1226DM	1226
V1277	Murphy-1
V1302	Proud
V1521	Murphy-2
V1539	Christmas
V1701New	V1701New
V1701New-B	V1701New
V2000	Dark Avenger 3
V2000-B	Dark Avenger 3
V2P1	1260
V2P2	V2P2
V2P6	V2P6
V2P6 Trash	V2P6
V2P6Z	V2P6
V920	Datalock
Vacsina	Vacsina
Variable	1260
Varicella	Npox.1482
VB Trackswap	Trackswap
Vbasic	Vbasic
VCL	Virus Creation Lab
Vcomm	Vcomm
VDIR	VDIR
Venezuelan	DenZuk

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description
Vera Cruz	Ping Pong
VF93	Virus Creation Lab
VFSI	VFSI
VGA2CGA	AIDS
VHP	Monxla A
VHP related (?)	Lisbon
VHP-348	VHP
VHP-353	VHP
VHP-367	VHP
VHP-435	VHP
Vien6	Vienna
Vienna	Vienna
Vienna 348	Vienna 348
Vienna 353	Vienna 353
Vienna 367	Vienna 353
Vienna 435	Vienna 353
Vienna 623	Vienna 353
Vienna 627	Vienna 353
Vienna 656	Lisbon
Vienna.Bua	BUTTHEAD
vienna family	C-544
Vienna variant	Monxla A
Vienna Variant	Monxla A
Vienna-B	Vienna
Vienna-B645	Vienna
Viki	Viki
Virdem 2	Burger
Virdem 792	Burger
Viresc	Jumper
Virus 101	Virus 101
Virus Creation Lab	Virus Creation Lab
Virus-90	Virus-90
Virus-B	Friday 13 th COM
Viruz	Viruz
Vlad the Inhaler	Vlad the Inhaler
Voice Master	Voice Master
Vootie	Vootie
Voronezh	Voronezh
Voronezh B	Voronezh
Voronezh-1600	Voronezh
VPT	Virus Creation Lab
W-13	Vienna
W13	Toothless
W13-A	Toothless
W13-B	Toothless
Warpcom-II	Warpcom-II
Warrier	Warrier
Wedding	Neuroquila
Welcomb	Buptboot
Welcomeb	Buptboot
Westwood	Westwood
Whale	Whale
Whisper	Tai-Pan
Wilbur	Wilbur
Wild Thing	IVP
Wildy	Wildy
Willow	Willow
WINSTART	WINSTART
WIPEOUT	DRPTR
Wisconsin	Wisconsin
Wllop	Sampo
Wolfman	Wolfman
Woodstock	Murphy-1
Wordswap 1385	Wordswap 1485
Wordswap 1485	Wordswap 1485
Wordswap 1504	Wordswap 1485
Wvar	Wvar
XA1	Christmas
Xph	Xph
Xtac	Xtac
Xuxa	Xuxa
xxx-1	Good Times
Yale	Merritt
Yankee Doodle	Yankee Doodle
Yankee Doodle 44	Yankee Doodle
YAP	Cascade
YB-1	YB-1
Year 1992	EUPM
yes	Dada
Yoshi?	Joshi
Youth	Youth
Z The Whale	Whale
Zapper (variant)	Stoned
Zaragosa	CAZ
Zaraza	3APA3A
ZBug	Zero Bug
Zeleng	Dark Avenger
Zero Bug	Zero Bug
ZeroHunt	ZeroHunt
Zerotime	Jerusalem
Zerotime.Australian	Jerusalem
ZigZag	ZigZag
ZIP Trojan	PKZIP Trojan 1
Ziploc	Virus Creation Lab
Zombie	Zombie

MS-DOS/PC-DOS Virus Name Cross Reference Table

Virus Name/Alias	Name in Description

Virus Name/Alias	Name in Description

Type Definitions Table

Type definitions: The type of a computer virus is a classification based on how it operates, how it infects files, or where it hides in memory.

Types	Description
Program.	A program virus attaches itself to a program and is activated when that program is run.
Boot sector.	A boot sector virus hides in the boot sectors of a floppy or hard disk. Viruses of this type also include those that hide in a hard disks partition table. A boot sector virus is activated whenever a machine is booted with an infected disk.
Companion program.	A companion program is a virus program with the same name as a .EXE program but with the .COM extension. Since .COM porograms are run before .EXE programs, the virus is executed first. After executing, the virus program runs the .EXE program to make it appear that nothing is wrong.
Directory structure.	A directory structure virus hides in the sectors normally used by a disks directory.
Bogus CODE resource.	The virus is added as a new CODE segment on the Macintosh, and the jump table is patched to point to that new segment. For example when an application is infected with nVIR, the virus attaches a CODE 256 resource to the end of the application and changes the CODE 0 resource (the jump table) to jump to and execute the CODE 256 resource before executing the application. Most Macintosh viruses (today) are of this type for example: Scores, nVIR, INIT29.
Patched CODE resource.	The virus code is added to the end of the main code segment on the Macintosh, and either the first program instruction or the jump table is patched to point to the virus code.
Bogus INIT.	A system INIT on the Macintosh is executed at boot time before the operating system takes over. They are used to patch the system and change its functionality, which makes them ideal for a virus.
Bogus resource.	Mac viruses of this type install a changed version of a standard system resource in the call chain between a program and the system. When a program needs a resource, it looks in the last opened file first, and then proceeds to the first opened file (the system) until it finds the resource it wants. The last opened file is usually a document, followed by the application, the desktop file, the finder, and the system. A viral resource placed on any of these files will be used in place of the one in the system file.
Trojan.	This isn't a virus, but a program that does damage of some sort that masquerades as something else. For example, DRAIN2 erases your hard disk while you play the game.
Worm.	This isn't a virus or a Trojan. A worm is a stand-alone program whose only property is to creates as many copies of itself as possible.
Virus Authoring Package (VAP).	A package that can be used to create new and different viruses.

Type Definitions Table

Vaporware Virus; not real.	This is a reported virus that turned out to be a hardware or software malfunction or a normal program acting in a suspicious way.
Macro.	A Macro virus uses a program's built-in macro capability to infect other documents. It is a document based virus, that generally is not platform specific.
Multipartite.	A multipartite virus infects more than one type of location on a disk, usually programs and the boot sector.
Other:	Programs that don't fit any of the other categories.

Features Definitions Table

Features definitions: The following table contains descriptions of virus special features such as how it hides from detection.

Features Types	Description
Direct acting.	A direct acting virus is one that only infects other files when the infected program is run. Trojans are also of this type. This is in contrast to memory resident programs that watch for triggers.
Memory resident; TSR.	A memory resident virus that loads as a TSR (Terminate and Stay Resident) program. A memory resident virus usually hooks some of the event traps from the operating system and uses those events to activate itself.
Memory resident; TSR above TOM.	A memory resident virus that loads at the TOM (Top of Memory). Most of these viruses then move the TOM down to make room for themselves, but a few don't. A memory resident virus usually hooks some of the event traps from the operating system and uses those events to activate itself.
Encrypted.	An encrypted virus has a small decryption segment, with the balance of the virus encrypted so key searches don't work.
Stealth; actively hides from detection.	A stealth virus uses one or more active methods to hide from detection programs. A common method is to make infected files appear normal when they are accessed by other programs such as DIR, or a virus checker (the 4096 virus is this type).
Polymorphic; each infection different.	Polymorphic viruses use different methods to hide each infection on a disk. They make each infection look different by using variable encryption, or modification of the object code by the insertion of No-OPs. They can be very difficult to locate with a signature scanner, because you must find an unchanging signature to scan for.
Retrovirus; attacks antivirus programs.	A reterovirus directly attacks antivirus programs and other programs that might detect its presence.

Features Definitions Table

Disk Locations Definitions Table

Disk locations definitions: The following table describes where viruses hide on disk.

Disk Locations	Description
Floppy disk boot sector.	The virus hides in the boot sectors of a floppy disk. The original boot sector is moved and executed by the virus after the virus finishes running. Data disks can also spread boot sector viruses.
Hard disk boot sector.	The virus hides in the boot sectors of a hard disk. The original boot sector is moved and executed by the virus after the virus finishes running.
EXE application.	The virus hides in .EXE executable files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
COM application.	The virus hides in .COM executable files, but not necessarily COMMAND.COM, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
COMMAND.COM	The virus hides in the COMMAND.COM system files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code. COMMAND.COM viruses also have hidden in some of the blank areas within the application, so they don't increase its length.
Program overlay files.	The virus hides in .OVL overlay files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.
Directory.	The virus hides in the sectors that normally contain the directory.
Hard disk partition table.	The virus hides in the partition table of a hard disk. The original partition data is usually stored in the virus or elsewhere and accessed by the virus when needed.
File Allocation Table (FAT)	The virus hides in the sectors that normally contain the file allocation table.
Bad blocks.	The virus stores itself on disk then marks the blocks where it hides as bad. A small fragment of the virus must be outside of the bad blocks to cause a jump to the code stored there.
Application programs and the Finder.	Most Mac viruses are transmitted by attaching to general applications, or to the Finder.
System program.	Most Mac viruses are passed from an infected application to the System, which then infects other applications.
INIT program.	INIT programs on the Macintosh run just after system startup to add functionality to the system. A virus posing as an INIT adds its own special functionality.

Disk Locations Definitions Definitions Table

Desktop file.	Some Mac viruses (WDEF) attache to the Desktop file, and intercept system resource requests, replacing them with the viral resource. These viruses can be passed without running an application, but merely by inserting an infected disk in a Mac (the Finder opens and reads the Desktop file whenever a disk is inserted).
Document files.	A virus attaches to a document file (this works only in a Mac, so far).
HyperCard Stack.	The virus hides in a HyperCard Stack (Mac).
SYS System files.	The virus hides in .SYS files, usually by attaching to the end of the application and placing a jump to the attached code at the beginning. After the virus code runs, it jumps back and executes the applications code.

Damage Definitions Table

Damage definitions: These are the types of damage that a virus may inflict on the attacked system. This damage in not necessarily intentional on the part of the virus writer, but often is caused by bugs in the virus program. Damage does not always occur, as most viruses rely on a damage trigger of some sort, since immediate damage prevents the spread of the virus. Triggers include dates, and the number of times an infected program is run.

Damage Types	Description
Corrupts a program or overlay files.	Most viruses spread themselves by attaching to an application, damaging it. Viruses may actively seek to destroy specific applications (SCORES). Other viruses write information to a specific block on a disk, which destroys any file that might already be using that block.
Attempts to format the disk.	This is usually an intentional attempt to destroy all information on a disk.
Interferes with a running application.	Interference can be intentional or caused by bugs in the virus. Intentional interference consists of things like making the letters fall in a heap at the bottom of the screen (Cascade), playing music at odd times (Oropax), or inserting typos when specific keys are pressed (Typo). Unintentional interference consists of bugs in the virus code that cause things like printing problems or crashes (nVIR, SCORES).
Corrupts a data file.	Data files are corrupted either by changing their contents, overwriting them with viral code, or deleting them.
Corrupts the file linkages or the FAT.	The file linkages, the File Allocation Table (FAT), and the file directory control where a file is on disk, and how the blocks of data that make up the file are linked together. Some viruses actively overwrite the FAT, since it is an easy way to corrupt a disk. Others, actually hide the viral code in the directory.
Attempts to erase all mounted disks.	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Encrypts the file directory.	The files themselves are still OK, but the directory entries are gone. The files are probably recoverable.
Erases the Hard Disk.	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Overwrites sectors on the Hard Disk.	Some viruses store things in specific sectors on the hard disk. If another file already used that sector, the file is destroyed. If the sector contains the FAT, directory or is the boot sector, all files may be lost.
Deletes or moves files.	The virus deletes or moves files on the disk.
Cracks/opens a BBS to nonprivileged users.	This is usually a Trojan with an inviting name that copies the user directory and password file to a directory where the virus writer can download it.
Erases a Floppy Disk	If files are simply erased, only the directory entries are lost and the files re recoverable. Other viruses encrypt the disk, which makes it unrecoverable (Disk Killer).
Corrupts floppy disk boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else. This can also occur on a nonsystem disk.

Corrupts hard disk boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else.
Corrupts hard disk partition table	The partition table tells the system where the logical disk drive is on the physical hard disk. The partition table includes code to be loaded into memory and used to do the actual partitioning of the disk. This code is loaded even before the system is booted, so a virus placed there gains control of the system before any virus protection software can be installed.
Corrupts boot sector	Boot sector viruses place their virus code in the boot area of a floppy disk, and usually move the boot code somewhere else.
OTHR This code is used for non-standard messages.	The code OTHR is used for non-standard messages where appropriate. It is not defined in this file so anything inserted as a description will not be replaced.
Does no damage.	This code does no damage at all, to any part of a machine.
No damage, only replicates.	This code does no damage either intentionally or unintentionally. It only replicates.
Unknown, not analyzed yet.	Unknown. The code has not been analysed in sufficient detail to know if it can do damage.
Trashes the hard disk.	Trashes the hard disk in some way. Probably by overwriting, encrypting, or formatting.
Trashes the floppy disk.	Trashes the floppy disk in some way. Probably by overwriting, encrypting, or formatting.
Damages CMOS.	The virus changes the CMOS settings either to make the computer unbootable, or to spoof a clean boot from a floppy while really booting from the hard disk.

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

List suggestions for improvement here.

Optional:

Name _____ Phone _____

Stamp

Computer Incident Advisory Capability
Lawrence Livermore National Laboratory
P.O. Box 808, L-303
Livermore, CA 94551

Department of Energy

CIAC

Computer Incident Advisory Capabil

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551